Error Correcting Codes for Distributed Systems on Arbitrary Channels

Thesis
Submitted for the award
of the degree of
Doctor of Philosophy

by
Uma Shankar Pandey

Under the Supervision of
Prof. P N Srivastava
Director, Institute of Systems and Computer Sciences

Department of Mathematical Sciences and
Computer Application
Bundelkhand University, Jhansi (UP)
2002

Certificate

This to certify that the work embodied in the thesis entitled "Error Correcting Codes for Distributed Systems on Arbitrary Channels" being submitted by Uma Shankar Pandey for the award of degree of Doctor of Philosophy to the Bundelkhand University, Jhansi, has been carried out by him under my supervision and guidance, that the work embodied has not been submitted elsewhere for the award of any other degree and is upto the mark both in its academic contents and quality of presentation.

He has put up attendance of more than 200 days with the supervisor in the department.

2/4/02

(Prof. P N Srivastava)
Head, Department of Mathematical
Sciences and Computer Application
Director, Institute of Systems and
Computer Sciences,
Bundelkhand University, Jhansi (UP)

Acknowledgements

Interdependence is not only a law of nature, it is also a reality of academic pursuits in any field. The knowledge flows from the feets of the Guru who dispels darkness and shows the way. I treat it my cherished privilege to express my gratitude and profound reverence for Professor P N Srivastava, Head, Department of Mathematical Science and Computer Applications, and Director, Institute of Systems and Computer Sciences, Bundelkhand University, Jhansi for his scholarly guidance and unstinted support throughout the study.

My heart bubbles offer its greatest thanks to my mentor Prof. Manahor Lal, Director, School of Computer and Information Sciences, Indira Gandhi National Open University (IGNOU) New Delhi, who paved my way to success by enlightened discussions, critical observations, discerning comments and constant inspirations. My friends particularly, Dr. D R Singh, Dr. Sanjai Bhatt, Dr. K V Joshi deserve special thanks for rendering friendly cooperation at various levels.

I wish to put on record the support received form the librarians of various libraries particularly from Dr. S C Jindal of Science Library, Delhi University and Dr. J P Singh of Defence Scientific Information and Documentations Centre (DESIDOC, Delhi). My thanks to many unknown persons who helped me through the Internet as well as the Library staff of Indian Institute of Technology, Delhi and Chennai.

I thankfully acknowledge assistance received from Mr. Harish Swamy who has done the typing and layout of the thesis meticulously.

I owe a sense of obligation to my parents who always wanted to see me on top of academic ladder. I have no words to pay their debt. I express my deep appreciation for my wife Kiran and kids (Kirti and Kovid) who have willingly allowed me to use family time for this task.

Uma shankar Pandey

Uma Shankar Pandey

April 2002

Table of Contents

List of Figures

CHAPTER I

INTRODUCTION

1.1 Development of Coding Theory

1.2 Communication System

1.3 Linear Codes

1.4 Channel (Mathematical Concepts)

1.5 Error Pattern and Coset Decomposition

1.6 Bounds on Number of Parity-Checks and Minimum Distance of Codes

1.7 Bursts Error Correcting Codes

1.8 Applications

1.9 Problems Discussed in this Thesis

CHAPTER I

Introduction

1.1 Development of Coding Theory

Digital information, its processing and communication are the dominant features of modern-day society. Digital information has become an asset not only to the educationist but also to people in all walks of life. Day by day, the human life is becoming more and more dependent on the computing and communication devices, in the form of computers, CD players, Modems, Routers, Gateways, Internet, Intranet, and on communication techniques using microwaves, telephone lines, and satellite communication systems. Figure 1.1 illustrates a modern communication network.

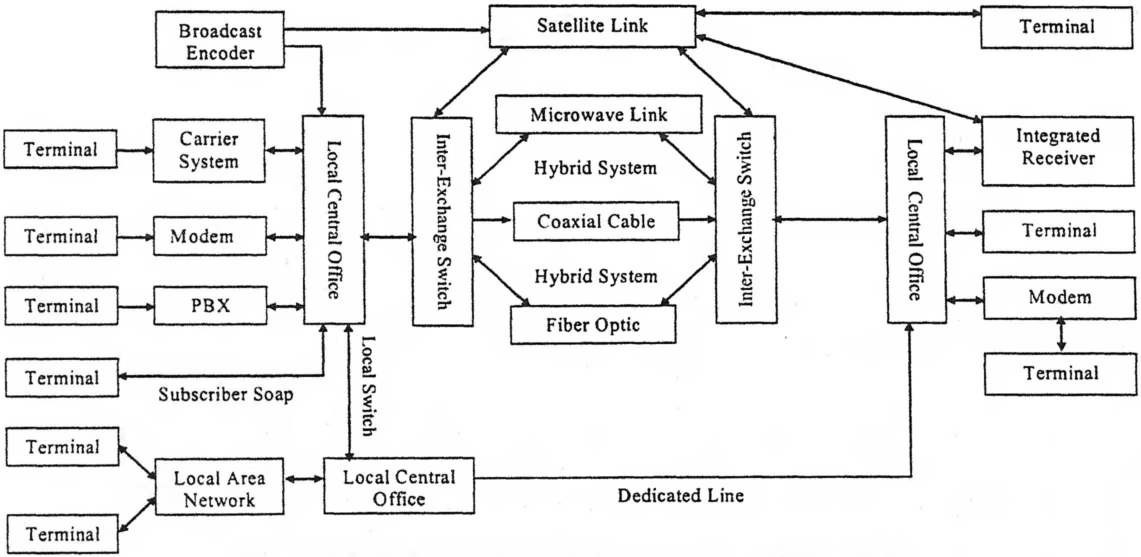


Figure 1.1: Modern Communication Network

Though the communication devices are highly reliable and still improving, yet because of disturbances in the environment in communication media, there is a likelihood of the corruption of the transmitted data, which may not be received as is transmitted. The discipline of error correcting/detecting codes deals with techniques for encoding the to-be-transmitted data and decoding the received data so that the possibility of error is minimised.

Shannon (1948) in his landmark paper "A Mathematical Theory of Communications" proved existence of error correcting/detecting codes, that under suitable conditions, and at rates less than the channel capacity would transmit error free information for all practical applications. For details we may refer Gallager (2001), which incorporates detailed discussion of the Shannon theory and his life achievements.

The theory of Error Correcting Codes was developed to achieve what is guaranteed by Shannon's fundamental theorem. However, to this day this aim of coding theory remains only partially fulfilled. Work in this area began with highly significant papers of Hamming (1950) and Golay (1949). The Classes of codes constructed by them present a very readable introduction to the philosophy of coding. Hamming (1950) introduced the basic concepts of *linear parity-check matrix* and a *metric.* Muller (1954) notion of *threshold decoding.* They also gave some preliminary observations in respect of using algebraic notations in coding theory. Then came one of the most important achievements of coding theory through the work of Bose and Choudhary (1960) and Hocquenghem (1959) independently, providing thereby a general method of construction of binary codes capable of correcting multiple random errors.

As the subject of error-correcting codes has arisen because of practical needs in the area of communication, it is important to evaluate the *Performance of a Code*[1]. In this direction earliest significant work has been done by Fano (1961), Gallager (1965), Shannon, Gallager and Berlekamp (1967). Minimum distance plays an important role in evaluating performance of codes. Notable contributions in terms of bounds on minimum distance have been made by Hamming (1950), Varshamov (1957), Gilbert (1952), Plotkin (1960), and Elias (refer, Peterson and Weldon, 1972).

McEliece-Rodemich-Rumsey-Welch (1977) used linear programming techniques to derive the best upper bound on minimum distance for large code lengths. *Perfect Codes*, which are the best codes in respect of

[1] The performance of a code is judged either in terms of probability of decoding error when the channel for which the code is designed, is specified or in terms of minimum distance for random errors when the channel is not satisfied or in general in terms of correctable error patterns.

the performance of codes, remained a puzzle for quite some time. Tietavainen (1973) and Tietavainen and Perko (1971) ultimately settled the question of existence of perfect codes for Hamming metric. In case where it is difficult to find out perfect codes for some values of parameters n and d next best alternative is to find out maximum cardinality code. Ostergard (1999) suggests a method of finding maximum cardinality q-ary codes, which are denoted by $A_q(n, d)$[2].

A large number of important code constructions, including those of BCH codes, use the *technique based on the roots of polynomials*, which have coefficients in a Galois Field. Mattson and Solomon (1961) introduced a new technique now termed as *associated polynomial approach* to coding. Recently, Cleju and Sirbu (1998) present a new method for code construction, which neither used matrices nor polynomials. This *implies the choice of codewords* one by one, by means of a special selection algorithm (computer implementable). Using this method they obtained binary, non-binary and burst error correcting block codes.

Shannon's theory has not only been a source of inspiration to the researchers in coding theory, but a source of frustration also, as for some

[2] $A_q(n, d)$ denote the maximum cardinality of q-ary code with length n and minimum distance d

time no one was able to construct a family of *Asymptotically Good Codes*[3]. It is the asymptotically good codes, which have more practical value than perfect codes. In this sense, even the otherwise very good class of BCH codes are found to be weak (refer Lin and Weldon, 1967). First partial success in obtaining asymptotically good codes was achieved by Elias (1954) by using *product code*[4].

Initially, major work in coding theory was in respect of only binary codes, however, the signified role played by *non-binary codes* in representing information much more concisely or economically, attracted the attention of researchers to non-binary codes. Though codes over non-binary alphabets have been designed for almost a decade, yet the metric used for these codes was similar to the one used for binary codes, namely Hamming Metric. Hamming Metric is the only possibility for binary codes. However in the case of non-binary codes there are many possibilities for metrics to suit various practical channels.

[3] Family of codes with error probability approaching zero and rate bounded away from zero, as guaranteed by Shannon.

[4] Let C_1 be an (n_1, k_1) linear code and C_2 be an (n_2, k_2) linear code, then an (n_1n_2, k_1k_2) linear code can be formed such that each code word is a rectangular array of n_1 columns and n_2 rows, in which every row is a code vector in C_1 and every column is a code vector in C_2, this two dimensional code is called product code of C_1 and C_2. (for details refer Lin and Costello, 1983)

Lee (1958) introduced first non-Hamming metric for non–binary alphabets known as Lee-metric, which is suitable for phase-modulation schemes. A number of good Lee-metric codes are presented in Berlekamp (1968) and in papers by Golomb and Welch (1968), Chiang and Wolf (1971) and Mazur (1973). Ahlswede, Bassalygo and Pinsker (1999) proved that for non-binary codes, generalized Hamming Bound is asymptotically sharp in some range of the code rate. Non-binary constant weight codes (CWC) play a very important role in coding theory in the sense that the decoding of such codes is relatively easy and less error prone. Svanstrom (1997) defined a lower bound on the size of ternary constant weight code. Fu, Klove, Luo and Wei (2001) generalized and improved the Svanstrom Bound. Duman and Kurtas (2001) develop *Union Bounds*[5] for high rate linear codes used for *partial response equalized channel* with additive white Gaussian noise.

Initially, major attention in coding theory has been devoted to the study of linear block codes correcting random errors due to noise in symmetric Hamming-metric channels. There have been significant contributions to other areas of coding theory also. MacKay (1999) defined MacKay-Neal codes which are shown to be "very good", in the sense that MacKay-Neal technique produces sequences of codes which, when optimally decoded,

[5] The Union Bound assumed uniform interleaving and based on an approximation,

achieve information rates up to the Shannon limit. This result holds not only for the binary-symmetric channel but also for any channel with *symmetric stationary ergodic noise.*

Linear codes have many practical advantages and are easy to handle in view of the applicability of algebraic tools. However, *non-linear codes* have the advantage of having the *largest number of codewords* possible for a given length. Vasilyev (1962) constructed a class of single-error-correcting perfect codes, which contains both linear and non-linear codes in its definition and Hamming codes as a subclass. Different mathematical tools have been used in the construction of practically used codes, Hadamard matrices also provide one such useful tool in construction of non-linear codes. Bose and Shrikhande (1959) and Plotkin (1960) constructed binary codes from Hadamard matrices. Semakov et. al. (1969) generalized these constructions to fields with q elements.

From practical experience, it was found that most of the errors that occur are in *bursts*. Abramson (1959), Reiger (1960), Melas (1960) laid the foundation for burst-error-correcting codes. The most successful early burst error-correcting codes were designed by Fire (1959). Forney

which is valid for high rate linear codes.

(1971) contains a survey of early work in this area. Later, further studies in this area were carried on by Farrell and Hopkins (1982), Daniel (1985), Blaum, Farrell and Tilborg (1986, 1988), Overfed (1987), Abdel-Ghaffar, McEliece and Tilborg (1988), Blaum (1990), and Zhang and Wolf (1990).

Further, from the point of view of coding and decoding efficiency, Knuth (1986) has designed a *Balanced Code*[6] containing unequal length codewords, and developed a coding schemes in which each code word contain equally many 0's and 1's. The main reasons given are *Serial Decoding Scheme*[7] with $k=2^r$ information bits and r check bits; and *Parallel Decoding Scheme*[8] with $k=2^r-r-1$ information bits and r check bits. The Parallel Decoding Scheme is much faster than the Serial Decoding Scheme. Al-Bassam and Bose (1990) show that balanced code with 2^r (or 2^r-1) information bits for *r* even (or *r* odd), where *r* is the number of check bits using parallel decoding scheme can be designed.

[6] Balanced Codes have the property that no code word is "contained" in another; i.e., the positions of the 1's in one codeword will never be a subset of the positions of the 1's in a different code.

[7] In Serial Decoding, the check represents the weight of the original information word. The decoding of the received word is done by complementing, first one bit, if required two bits, if further required three bits and so on until the weight of the information word is equal to the values represented by the check.

[8] In Parallel Decoding Method, the check directly indicates the number of information bits complemented and hence at the decoder side the original information word can be obtained by complementing this number of bits in parallel i.e., all these bits can be complemented simultaneously.

These codes are very useful in encoding of unchangeable data on laser disk.

Spielman (1997) presented a new class of asymptotically good, linear error-correcting codes. Codes, which can be both, encoded and decoded in linear sequential time and logarithmic parallel time with a linear number of processors and which present both randomized and systematic constructions of these codes. Another important step in the construction of such codes is the introduction of error *Reducing Codes*[9].

In many space and satellite communication systems *Convolutional Coding*[10] with *hard-decision*[11] and *soft-decision*[12] viterbi decoding has been applied. Viterbi decoding of convolutional codes can also be used in concatenate coding scheme with Reed-Solomon code. Unit Memory Convolutional (UMC) Codes were introduced by Lee (1976) and Lauer (1979) which were found to be an interesting alternative to the usual

[9] Reducing Codes are codes, which have a decoder that can very quickly remove a constant fraction of the errors from a corrupted codeword.

[10] The set of encoded sequences produced by a k-input, n-output encoder of memory order m is called an (n, k, m) Convolutional Code (refer Peterson and Weldon, 1972).

[11] In a Hard-decision decoding the receiver decides whether each transmitted symbol is a 0 or a 1 and the received vector is a binary (0 or 1) sequence.

[12] In a Soft-decision decoding the receiver generates some analog information on each received symbol and the decoder recovers the message from the analog or quantized received vector.

convolutional codes, as they can have larger free-distance than the usual *multi-memory convolutional codes* (MMC) with the same rate and the same number of memory elements in the encoder. It is useful because their block length can be chosen to agree with the word length of computers or microprocessors that are used in the decoding and encoding equipment. Lee gave a table of short UM codes and a single upper bound on their *Free Distance*[13]. Thommesen and Justesen (1983) studied the distance property of UMC and derived their upper and lower bounds. These bounds indicate that in many cases of interest, UMC may be expected to have superior properties. Justesen, Paaske and Ballan (1990) suggest a class of UMC codes that are defined by generator matrices composed of circulant sub-matrices and are better in the sense that the structure of these codes facilitates the analysis as well as an efficient search for good codes. In analogy with the well-known class of block codes, they refer to these codes as *Quasi-Cyclic UMC* (QCUMC). Forger (1995) described a new construction of Unit Memory Code that are based on Reed Solomon Code having the same free-distance.

Thinking about coding and its effect on *bandwidth* was quite a revolutionary idea given by Ungerboeck. It is probably fair to say that the *Trellis Coded Modulation* (TCM) schemes suggested by Ungerboeck (1982,

[13] Free Distance is defined at page 27.

1987), captured the attention of the modulation community and inspired wide-spread practical applications as well as intensified the research in this area. Ungerboeck showed how coding gains of order 3 dB could be obtained with a simple four state codes. Calderbank and Sloane (1986), developed eight dimensional trellis codes and a new class of trellis codes based on the concept of Lattice and *Coset*[14].

Wei (1987)[15], developed trellis coded modulation with multidimensional *Constellation*[16] and schemes that performed better for the same complexity than two-dimensional schemes. Survey in this respect by Forney (1988) is quite useful. Dillcen and Lindsey (1997) presented a new and novel technique known as *Codec*[17] (coder-decoder) which combines trellis coding with an *m*-ary orthogonal modulation for application in *Wideband Channels.* The novelty of the technique lies in the fact that current popular coding schemes which combine coding and modulation, such as trellis coded modulation (TCM), have only been applied to *Narrowband Channels.*

[14] Development of coded modulation scheme for band-limited channels.

[15] This paper has been awarded "The Information Theory Society Award" in 1987.

[16] Such schemes involve selecting sequence of signals from redundant signal sets.

[17] The Codec provides satisfactory bit error rates at lower transmitted signal power levels.

Linear block codes can be designed to have powerful error-correcting, and error-detecting capabilities, and can be encoded and decoded efficiently due to their elegant algebraic structures. However, they usually possess undesirable *DC-Properties*. *Line codes* (or transmission codes) on another hand are designed to have a zero dc-component and limited *Run Length*[18] to aid in the receiver synchronization and detection processes, but typically offer little or no error-control capabilities. The dc-free attribute can be achieved by strongly bounding the running disparity of the transmitted sequence. The disparity of the codeword is the difference between the number of 1's and the number of 0's. Deng and Herro (1988) constructed a class of codes, which met the dc-constraint and the error-correcting requirements. Because of the simplicity of encoder and decoder design it can be used for high-speed digital communication. Further, Oreilly and Popplewell (1990) corrected and refined the disparity and run length or Running Digital Sum (RDS). Later, Jeong and Joo, (2000), by using Trellis and multilevel code structure defined a class of DC–free codes. Chiu (2001) proposed a new construction of DC–free error-correcting codes based on convolutional codes. The new codes constructed by selecting a proper sub code from a convolutional code composed of two different component codes. The

[18] The Run Length is defined as the number of consecutive 1's or 0's in sequence of coded bits.

encoder employs a Viterbi algorithm as the codeword selector so that the selected code sequences satisfy the DC constraint. A lower bound on the free distance of such codes is proposed, and a procedure for obtaining this bound is presented.

One of the major goals of the research in coding theory, in recent decades, has been to develop codes that had large block lengths, yet contain enough structure that practical decoding was possible. A new encoding and decoding scheme, called *Turbo Codes*[19] was introduced by Berrou, Glavieux and Thitimasjshima (1993). Turbo codes achieved near capacity performance on an Additive White Gausian-Noise (AWGN) channel. It appears that four-decade effort to reach channel capacity was achieved by this latest discovery. For sufficiently large message-sequence block length, a performance which is very close to the Shannon limit can be achieved at a moderate bit-error rate (BER), even though the free distance of the turbo codes is not large. Hagenauer (1997) defined in detail the turbo principles. Hall and Wilson (2001) explored a stream paradigm for turbo codes termed stream-oriented turbo codes. Dejonghe and Vandendorpe (2001) introduced the methods and fundamental principles associated with the decoding scheme of the turbo codes and

[19] Turbo Coding is a channel coding scheme base on the concatenation of convolutional codes along with interleaving and iterative decoding rule.

show that it is possible to extend these methods and principles to other problems frequently encountered in digital communications. They also defined turbo equalization and turbo Multiuser detection.

Efficient codes based on graphs have also been designed. Ping, Huang and Phamdo (2001) introduced a family of error-correcting codes called zigzag codes. A zigzag code is described by a highly structured zigzag graph. Due to the structural properties of the graph, very low complexity decoding rules can be implemented. They present a decoding rule, based on the Max-Log-APP (MLA) formulation, which requires a total of 20 addition-equivalent operations per information bit, per iteration. A union bound analysis of the bit error probability of the zigzag code is also included. Further, it is shown that the union bounds for these codes can be generated very efficiently. It is also illustrated that, for a fixed *Interleaver*[20] size, the concatenated code acquires increased code potential as the number of constituent encoders increases. The analysis shows that zigzag codes with four or more constituent encoders have lower error floors than the comparable turbo codes with two constituent encoders have.

[20] Interleaving is the method of for breaking up a burst into shorter ones and making detection or correction of the burst easier.

Codes have been studied and constructed, not only for communications purposes only, but also to maintain consistency of storage, components of computers, and even for any general finite state machines. For applications in computer memory system, Chen (1985) presented the construction of a class of linear codes capable of masking some memory defects and correcting multiple random errors. Pollara, McEliece and Abdel-Ghaffar (1987) defined a class of codes called finite-state (FS) codes. These codes, which generalise both block and convolution codes, are defined by their encoders, which are finite state machines with parallel inputs and outputs.

The codes discussed so far have been about correction/detection of only bit errors whether random or in the form of bursts. However, codes for correcting random or burst of *bytes* have been found useful in practical applications. Chen (1986) developed techniques for the construction of error-correcting codes for semi conductor memory subsystem that can be organised in a multibit-per-chip manner. These codes (SBC-DBD) are capable of correcting all single byte errors and detecting all double-byte errors, where a byte represents the number of bits that are fed from the same chip to the some codeword. Zhen (1993) presented a new approach to the construction of systematic tEC/AUED (t-error correcting and all unidirectional error-detecting) codes. These new constructions improve many of the upper bounds of the redundancy of the codes.

Farrell and Tandon (1997) designed powerful classes of Error Detection and Correction (EDC) code, for multitrack recording channels and used the Reed Solomon Block Symbol Codes. It is particularly effective with Reed Solomon codes to use a powerful technique known as interleaving which alters the number of error symbols within a block and can therefore improve error performance. Important parameters that influence the efficiency and cost effectiveness of such codes include block size, interleave depth and the power of the symbol correcting code. Using error performance, estimation techniques allow a designer to experiment with these parameters to produce efficient EDC codes.

Feng and Rao (1997) constructed a class of double-byte error- correcting codes, which are more efficient than the previously known codes. Single-byte error correcting and double-byte error-detecting (SbEC-DbED) codes have been successfully used in computer memory Subsystems. Chattopadhyay and Chaudhuri (1997) gave a new design scheme which has been reported for parallel implementation of SbEC/DbED code that is analogous to the convolutional Reed-Solomon code.

For providing a reliable communication link to real-time systems, and data and voice services. Chan and Geraniotis (1997) designed a *type-II* *adaptive hybrid*[21] *FEC*[22]*/ARQ*[23] protocol using Turbo codes. For the purpose, a powerful family of Error Correcting Codes using parallel concatenated Convolutional codes is introduced. Near-Shannon-limit is achievable by such codes. Given the promising performance of the codes, it is expected that the performance of an adaptive FEC/ARQ protocol employing turbo codes will be better than protocols using other Error Correcting Codes. For real-time services, the number of retransmissions is limited to one so as to limit the delay. For data services, the number of retransmissions is unlimited to provide a reliable communication link. Results in terms of throughput obtained through analysis and approximation using the performance curves are encouraging.

Prasad and Seki (1997) analysed the performance of a hybrid selective repeat (SR)/multi copy (MC) automatic repeat request (ARQ) scheme to transmit fragmented Internet Protocol (IP) packets. The ARQ scheme works in SR mode till the last IP packets fragment is transmitted. If a packet is negatively acknowledged after the last fragment is transmitted

[21] Type-II of hybrid scheme is devised based on the concept that the parity-check digits for error correction are sent to the receiver only when they are needed.

[22] Forward Error Correction (FEC) is the technique is which the transmission errors are corrected at the receiving end by applying an error correcting code.

[23] Automatic Repeat Request (ARQ) is the scheme to request the retransmission of data when the receiving end detects the transmission errors by using the error correcting code.

then the system goes in MC mode. In MC mode multiple copies of the erroneous fragment are transmitted. After all fragments are received without error the system goes back to SR mode. Performance of the ARQ is evaluated in terms of BER, IP packet size and fragmentation size. Performance results are also obtained using Bose Chaudhari Hocquenghem (BCH) error correction codes.

For digital cellular multiple access system Ericson (1988) introduces the concept of superimposed codes in Euclidian n-space R^n, which is very useful in multiple access communication. Saleki (1989) invented *Optical Orthogonal Codes*[24], the use of which enables a large number of asynchronous users to transmit information efficiently and reliably and can be used in a code-division multiple-access fibre optic channel, mobile radio, radars and speed-spectrum communication. Kuhn, Dekorsy and Kammeyer (2000) investigate aspects of channel coding in *Code Division Multiple Access*[25] (CDMA) systems. This inherent bandwidth expansion requires the application of powerful low rate codes

[24] Optical Orthogonal code is a family of (0,1) sequences with good auto and cross correlation properties i.e., the autocorrelation of each sequence exhibits the "thumbtack" shape and the crosscorrelation between two sequences remains low throughout. The thumbtack shaped autocorrelation facilitates the detection of the desired signal and low-profiled crosscorrelation reduces interferences from unwanted signals.

[25] CDMA is a system where each user occupies a bandwidth much larger than the information bit rate.

with low decoding complexity. In this context, three different *Coding Strategies*[26] have been considered.

For reference and detail study in the area of error correcting/detecting codes, there are many books, monographs, collection of papers and surveys. Notable among books are by Peterson and Weldon (1972), Berlekamp (1968), Lin and Costello (1983), Blahut (1987), Golumb (1964), Hamming (1980), Hill (1986), Imai (1990), Reed and Chen (1999), Hoffman eds. (1991), Lint (2000), Pless (1989), Rao and Fujiwara (1989), Wicker (1985), MacWilliams and Sloane (1988), and Rhee (1989). Important papers are Forney (1971), Blaum (1985, 1987), Chen (1983, 1985), Reed (2000), etc.

1.2 Communication System

Whatever may be the techniques and tools of communication system whether it is satellite, optical fibre or micro wave based, the basic component of a communication system can be represented as shown in Figure 1.2, which is a simplified model of communication system using block diagram.

[26] The combination of convolutional and repetition code; the code-spread system consisting of a single very low rate convolutional code; and a serial concatenation of convolutional Walsh-Hadmard and repetition code.

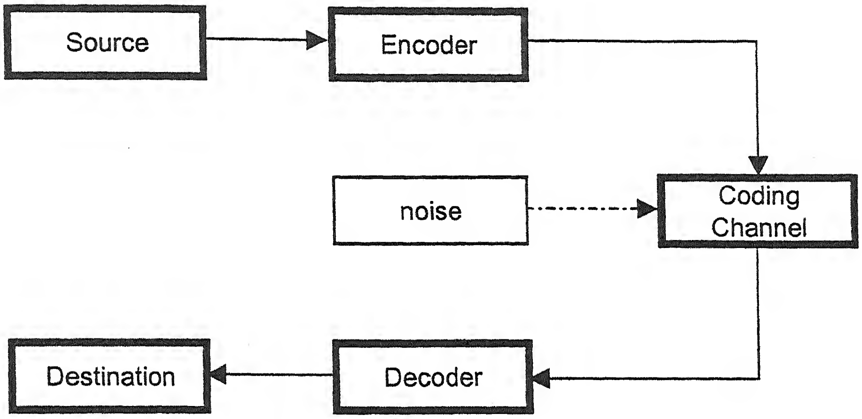


Figure 1.2: Simplified Model of Coded System

Source: Source produces a message or sequence of messages to be communicated to the receiver. The source output might represent, for example, a waveform, a sequence of binary digits, the output of set of sensors in a space probe, a sensory input to a biological organism, or a target in a radar system.

Encoder: Encoder represents any processing of the source output prior to transmission. The processing might include, for example, any combination of modulation, data reduction and insertion of redundancy to combat the channel noise.

Channel: Channel is a medium for transmitting signals from a transmitter to a receiver, it may be a twisted-pair telephone lines, a high frequency radio link, micro wave links, coaxial-cable wires, optical fibers, Satellite links, Space communication links. A typical storage medium are semiconductor memories, magnetic tapes, magnetic disks, compact disk (CDs) optical memory units, digital video disks (DVDs). The channel is usually subject to various types of disturbances called noise. However, all these physical channels can be represented by *Mathematical Concepts of Channel.*[27]

Decoder: Decoder represents the processing of channels' output with the objective of producing, at the destination, an accepted replica of the output.

Destination: Destination or the receiver is the person or object, maybe a computer or communication system for whom/which the message is intended.

1.3 Linear codes

There can be various ways of coding a source. In general this is handled through code characters, which form a finite set. For algebraic studies, which are quite adequate for logical implementation, the code characters are taken as elements of a finite field or more generally that of a finite ring. However, in our studies, the nature of the metric that we will be

[27] Refer 1.4 for Mathematical concepts of channel.

defined and employed in problems related to corrections of errors in this thesis, is modular (Berlekamp, 1968). Therefore, we will be confining to Z_q the ring of integers mod q. In most of the results in this thesis, q will be taken to be a prime integer, so that Z_q is a finite field.

Words can be formed from code characters. Most of the structures in the study of error-correcting codes deal with situations in which all of the words are taken as blocks of same length. We will be restricting to this framework of studies.

Algebraic structure over a code makes it easier to grasp the whole of the code from a much smaller subset of the code. The most commonly used codes are the linear codes, which are linear spaces over some suitable finite field. More specifically:

Linear Code: linear code of length n is a subspace of the space of all n-tuples over a finite field GF(q). As mentioned earlier, in this thesis, the finite field is taken as $Z_{q,}$ for a prime integer q.

If the dimension of the code as a linear space over GF(q) is k then we refer to this code as an (n, k) code also. In this case the number of code words, i.e., words in the code is exactly q^k.

Linear codes are best described in terms of generator matrices and parity-check matrices, which are defined as:

Generator matrix: A matrix G is said to be a generator matrix of a linear code if the row space of G is the given code.

Parity-check matrix: A matrix H is said to be the parity-check matrix of a linear code if the code is the null space of the matrix H.

If H is a parity-check matrix of a linear code C, then an n-tuple $\underline{u}$ is a code word if and only if $\underline{u}$ is orthogonal to every row of H, i.e.,

$$\underline{u} H^T = \underline{0} \Leftrightarrow u \in C \tag{1.1}$$

Syndrome of an n-Tuple: For an n-tuple $\underline{u}$, $\underline{u}H^T$ is called the syndrome of the n-tuple $\underline{u}$.

In an (n, k) linear code, k positions can be arbitrarily assigned values and are called **information positions** while the remaining n-k positions are determined by a set of rules or equations and are called **parity-check positions**.

Weight and Distance (Metric)

The notions of weight and metric are important concepts in the study of random error-correcting codes. Berlekamp (1972) has rightly pointed out that the notion of weight distinguishes the theory of linear codes from classical linear algebra. Depending on modulation scheme, there can be several ways of defining the weight of a vector and the distance between two vectors. However, mainly two types of weights/distances given by Hamming (1950) and Lee (1958) have been used in coding theory.

In the case of definitions due to Hamming, the code characters can be from an arbitrary finite set. But in the definitions due to Lee, the code characters are taken from the ring Z_q of integers mod q.

The definitions of weight and distance due to Hamming and Lee are taken up below.

Hamming Weight and Distance

Until or unless it is explicitly mentioned otherwise, a code would be considered over a field GF(q) where $q=p^s$ for some prime p with s being a natural number.

The **Hamming weight** of a vector $x=(x_1, x_2, \ldots x_n)$ denoted by w(x), is the number of non-zero components of x. Each component x_i is an element of GF(q). Further the vector x is also called an n-tuple or a word.

The **Hamming distance** between two vectors x and y, denoted by d(x, y) is the Hamming weight of the vector x–y. It also equals the number of positions in which the two vector differ. That is

$d(x, y) = w(x-y) = w(y-x)$

= the number of positions that x and y differ.

Lee Weight and Distance

The Lee weight of an n-tuple $(a_1, \ldots, a_n)$, a_i being chosen from Z_q, is defined as

$$w_L(\underline{u}) = \sum_{i=1}^{n} |a_i|_L ,$$

$$\text{where } |a_i|_L = \begin{cases} a_i , & 0 \le a_i \le q/2; \\ q - a_i , & q/2 < a_i \le q-1 \end{cases} \qquad \text{...(eq 1.2)}$$

The *Lee Distance* between two n-tuples is defined as the Lee-weight of their difference, i.e., Lee distance between n-tuples $\underline{u} = (a_1, \ldots, a_n)$ and $\underline{v} = (b_1, \ldots, b_n)$, a_i, b_i being chosen from Z_q is given by

$$d_L(\underline{u}, \underline{v}) = w_L(\underline{u} - \underline{v}) = \sum_{i=1}^{n} w_L|a_i - b_i|$$

$$\text{where } W_L|a_i - b_i| = \begin{cases} w_L(a_i - b_i) & \text{if} \quad a_i \ge b_i \\ w_L(q - (a_i - b_i)) & \text{if} \quad a_i < b_i \end{cases}$$

For q = 2 and 3, Lee weight of an n-tuple coincides with its Hamming weight. Therefore, in situations where studies are first made with reference to Hamming metric and subsequently with reference to Lee metric for q a prime integer, then in the latter case we will be considering q an *odd* prime only.

Apart from imposing the ideas of weight and distance over n-vectors, we associate these notions with a code also.

Minimum Weight of a Code: The minimum weight (Hamming, Lee or any other) of a code is defined as the minimum of weights of the non-zero words in the code.

We may generalise the concept of minimum weight of a code, which is linear and block to a non-linear code, which may not be block code.

Minimum Free Distance of a Code: The minimum free distance of code is defined as the minimum of distances between all pairs of distinct code words.

The minimum free distance d_{free} is defined as

$$d_{free} \underline{\underline{\Delta}} \min\{d(v', v''): u' \neq u''\}$$

where v' and v" are the code words corresponding to the *information sequences*[28] u' and u", respectively. It is assumed that if u' and u" are of different length, zeros are added to the shorter sequences so that their

[28] The source encoder transforms the source output into a sequence of binary digits (bits) is known as Information Sequence.

corresponding code words have equal length. Hence d_{free} is the minimum distance between any two code words in the code.

$$d_{free} = \min \{d(v', v'') : u' \neq u''\}$$

In the case of linear codes, minimum (free) weight and minimum (free) distance of a code coincide.

The notions of weight and distance help us in analysing the error correction capabilities as well as in proposing decoding procedure for the code. In this connection we state two basic results from theory of error-correcting codes.

1. A code with minimum distance at least 2t+1 is capable of correcting any combination of t or less errors in a code.
2. If a code C has minimum Hamming distance at least d then every combination of d-1 or less columns of the parity-check matrix of C is linearly independent.

A more general statement on error detection and correction has been given as follows:

A code can correct any combination of t errors and detect upto d errors ($d \geq t$) if and only if the minimum distance d for the code is $\geq t + d + 1$.

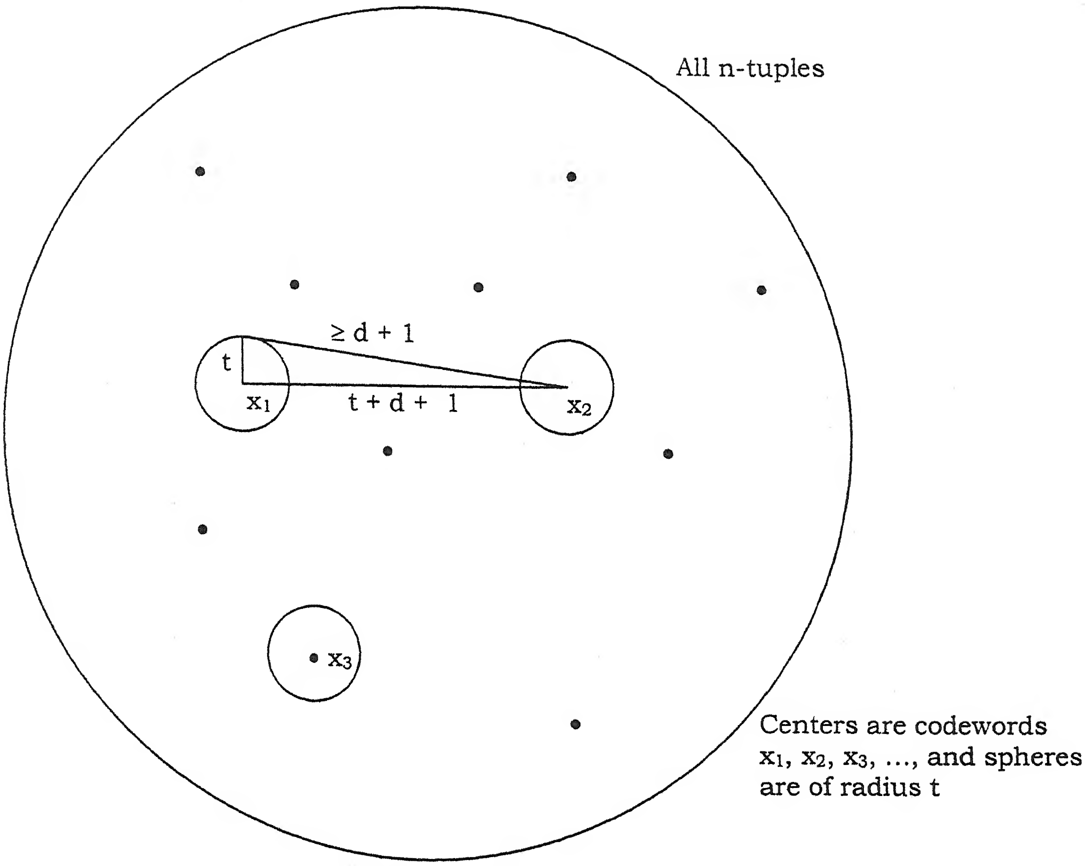


Figure 1.3 Illustration of Error Correction/Detection using Spheres Around Code Words

The proof of these results may be visualised by the pictorial representation as given in figure 1.3.

The Hamming and Lee distances are well suited respectively to orthogonal modulation schemes and phase-modulation schemes (c.f. Berlekamp, 1958). But there exist channels (e.g. those using amplitude modulation schemes against additive gaussian noise) to which neither of the two distances suit completely. This fact necessitates search for more metrics.

Golomb (1969) has given a nice formulation of the problem of error correction in terms of a general metric.

1.4 Channel (Mathematical Concepts)

Given two non-empty sets A and B to be called respectively the *input alphabet* and *output alphabet* and an arbitrary set S called the set of states, a channel is an ordered triplet

$$\left(A, B, \{p_n(b_1, b_2, \ldots\ldots, b_n \mid a_1, \ldots, a_n; s) : a_i \in A, b_i \in B \text{ and } s \in S\}\right),$$

Where $\{p_n\}$ is a system of probability functions satisfying

i) $P_n(b_1, \ldots, b_n \mid a_1, \ldots, a_n; s) \geq 0$ for all n,

$a_1, \ldots, a_n; b_1, \ldots, b_n$; s and

ii) $\sum_{b_1, \ldots, b_n} P_n(b_1, \ldots, b_n \mid a_1, \ldots, a_n; s) = 1$ for all n, $a_1, \ldots, a_n$, s.

We can interpret $P_n(b_1, \ldots, b_n \mid a_1, \ldots, a_n; s)$ as the probability that the sequence $b_1, \ldots, b_n$ will appear at the output if the input sequence $a_1, \ldots, a_n$ is applied and the state of the channel before the appearance of a_1, is s. Thus, in general, the state of the channels may change after each component of the input sequence is transmitted. In this model, knowledge of initial state and input sequence determines the distribution of the output sequence. However, here we restrict to the **discrete, memoryless, symmetric channels**. It may be recalled that

A channel is said to be **discrete** if both the input alphabet

A and the output alphabet B are finite sets.

Further a discrete channel

$$(A, B, \{p_n(b_1, \ldots, b_n | a_1, \ldots, a_n; s): a_i \in A, b_i \in B \text{ and } s \in S\})$$

is said to be **memoryless** if

1. The functions $p_n(b_1, \ldots, b_n | a_1, \ldots, a_n; s)$ are independent of s; hence may be written as $P_n(b_1, \ldots, b_n | a_1, \ldots, a_n)$; and

2. $P_n (b_1, \ldots, b_n | a_1, \ldots, a_n) = P_1(b_1 | a_1) \ldots P_1(b_n | a_n)$

For all $a_1, \ldots, a_n \in A$; $b_1, \ldots, b_n \in B$ for all $n = 1, 2, \ldots$

In other words, for a discrete channel to be memoryless, it is required that successive symbols are acted upon independently and the transmission probabilities do not depend on the state s.

Also a discrete, memoryless channel

$$(A, B, \{p(b_j \mid a_i): a_i \in A, \text{ and } b_j \in B\})$$

is said to be **symmetric** if the set $\{p(b_j | a_i)\}_{j=1}$, of probabilities of receiving $b_1, \ldots, b_j, \ldots$ for each transmitted a_i are equal for all i and the sets $\{p(b_j | a_i)\}_{i=1}$, of probabilities of receiving b_j when $a_1, \ldots, a_i, \ldots$ are transmitted, are equal for all j.

Decoding Schemes: One of the purposes of studies in coding theory is to achieve reliable communication over noisy channels. For this, after studying the behaviour of the channel, if the channel is given or otherwise if the channel is not given, we must be able to determine the transmitted code word from the received word with a high degree of accuracy. Thus we should have a rule, which associates a code word with each received word. This rule is called a decoding rule (or decoding scheme). More precisely,

A *decoding scheme* is a rule, which associates at most one code word with each received word.

A decoding scheme, which does not associate any code word with a received word, which is different from a code word, is useful in situations where the code word can be transmitted easily.

In a one-way communication system, mostly a scheme has to be adopted to every received vector, a code word is to be associated.

The following two schemes are mostly employed:

Maximum Likelihood Decoding Scheme (MLD): Given all code words are equally likely, a rule that chooses the code word having the *highest conditional probability* of being transmitted, for each received vector $\underline{v}$, is called maximum-likelihood-decoding scheme.

A brute force application of this rule requires comparing the received vector $\underline{v}$ with all the q^k code words in an (n, k) code over GF(q). This is fine for small codes. But for large q and k the task is almost impossible. As, one of the aims of coding theory is to find codes, which can be decoded by a faster method; for large q and k some other decoding methods should be applied. Another decoding scheme called *bounded distance decoding,* which is a modification of the maximum-likelihood-decoding rule, decodes if and only if the noise on the channel is not too large.

More precisely, according to *Bounded Distance Decoding* (BDD) a received vector $\underline{y}$ is decoded only if there is code word $\underline{x}$ at a distance not exceeding t, where t is a pre-assigned number. Otherwise $\underline{y}$ is not decoded. This decoding rule is usually applied in the case of algebraic codes.

Matching of a Channel and a Metric: Next, we define the notion of suitability of a metric to a channel. The definition is with reference to a decoding scheme. Thus, corresponding to each of the two decoding schemes defined in this section, we have

Definition: A metric and a discrete memoryless channel are said to be *matched for maximum likelihood decoding* (MLD) if the decoding rule "decode the received vector to the nearest (or farthest) code word" always gives a most probable code word.

Definition: A metric and a discrete, memoryless channel are said to be *matched for bounded discrepancy decoding* (BDD) if the decoding rule "decode the received vector to the code word which is with in a distance of t or less", where t is an integer smaller than half of the minimum distance between all pairs of code words, gives (whenever a decision has been made) a most probable code word.

The above definitions as given in Chiang and Wolf (1971), are respectively due to Massey (1967) and Wyner (1965).

These concepts have been further modified to those of *strictly matching* in Chiang and Wolf (1971). We take up these below:

Definition: A metric and a discrete memoryless channel are strictly matched for MLD if

$$w(E) < w(E') \qquad \text{if} \qquad p(E) > p(E')$$

Where E, E' are error vectors and w(E) and p(E) denote respectively the weight and probability that an error vector coincides with E.

Definition: A metric and a discrete memoryless channel are *strictly matched for BDD of radius t*, if

$$w(E) \leq t \text{ and } w(E') \geq t+1 \text{ then } p(E) > p(E'),$$

where E, w(E) and p(E) are defined as given above, and t is a non-negative integer.

Matching of channels to a general metric is discussed in the next chapter where the concept of general metric is defined.

1.5 Error Pattern and Coset Decomposition

When messages are transmitted over a noisy channel, these are not received as such. The noisy channel adds an error vector to it.

Error Vector: If the n-vector $\underline{v} = (b_1, \ldots, b_n)$ is received when n-tuple $\underline{u} = (a_1, \ldots, a_n)$, is transmitted then the difference n-vector $\underline{e} = \underline{u} - \underline{v} = (b_1\text{-}a_1, \ldots, b_n\text{-}a_n)$ is called an error vector (or an error pattern).

Since

$\underline{u}H^T = \underline{0}$

it follows that $\underline{v}H^T = \underline{e}H^T$

Thus the syndrome of a received vector is equal to the syndrome of the error vector added to the transmitted word.

Coset Decomposition: A coset decomposition of the space of n-tuples over GF(q) with respect of its subspace (the code) C is useful in formulating many results in coding theory. It is a simple proposition of algebra that decomposition of the space of n-tuple over GF(q) into cosets is complete and unique in the sense that every n-tuple over GF(q) is in one and only one coset. All n-tuples in a coset have some syndrome.

Weight of a Coset: The weight of a coset is defined as the minimum of the weights of n-tuples in the coset.

For an (n, k) linear code the number of cosets is q^{n-k} and hence at most $q^{n-k} - 1$ nonzero error patterns that belong to different cosets can be corrected.

1.6 Bounds on Number of Parity-Checks and Minimum distance of a Code

In this section all bounds are discussed with respect to

Hamming Metric only. A code should use minimum number of parity checks while keeping its error-correction capabilities intact. But it is not always possible to determine the exact number of parity checks. Therefore, we need to have bounds over them. We mention below some of the important bounds.

Hamming Sphere-Packing Bound

This bound obtained by Hamming (1950), states:

If an (n, k) linear code over GF(q), a galois field with q elements, is Capable of correcting t or less (Hamming) errors then

$$n - k \geq \log_q \left[1 + \binom{n}{1}(q-1)) + \cdots + \binom{n}{t}(q-1)^t \right]$$

A refinement of this bound was obtained by Wax (1959). Plotkin (1960) has obtained some close bounds and relations over minimum distance and number of parity checks for linear/non-linear block codes. Other important contributions in this area have been, among others, by Helgert and Stinaff (1973), Shrikhande (1962), Johnson (1971) and Bambah, Joshi and Luther (1961).

Plotkin Bound

Plotkin (1960) derived a necessary lower bound on number of parity checks by employing the technique of taking average. The bound states:

If $n \geq \frac{(qd-1)}{q-1}$, the number of parity checks required to achieve minimum weight d in a n-symbol linear block code is at least $\left[\frac{(qd-1)}{q-1}\right] - 1 - \log_q d$.

Varshamov-Gilbert Bound

A general lower bound on the number of code words in a code with given length and minimum distance was given by Gilbert (1952) and Varshamov (1957) independently. This states:

A sufficient condition for the existence of an (n, k) linear code-over GF(q) with minimum Hamming distance at least d is that n, k, q and d are such that they satisfy the inequality

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i$$

Sacks (1958) gave a method to obtain the above-mentioned bound, by constructing a parity-check matrix for the desired code.

Chapter 13 of Berlekap (1968) contains a general treatment of bounds, valid for Lee-metric codes also.

1.7 Burst-Error-Correcting Codes

Most work in coding theory has been addressed to efficient communication over memoryless channels, i.e., channels which add random errors to messages. While this work has been directly applicable to space channels (refer Ferney, 1970), it has been of little use of all other real channels, where errors tend to occur in bursts.

The work in the direction of burst error was initiated by Abramson (1959) who laid down the procedure for correcting all single and double-adjacent errors in the binary case. Later, Fire (1959) studied the subject for general burst. Further work of burst error correcting codes can be found in Campopiano (1962). Forney (1971) contains a survey of work in this area. Studies of linear burst error correcting codes have been nicely treated by Peterson and Weldon (1972). Further Farrell and Hopkins (1982) defined burst error correcting array codes and developed decoding algorithms for a class of burst error correcting array codes. Daniel (1985) defined double burst error correcting codes. Blaum, Farrell and Tilborg, (1986, 1988), presented a family of burst error correcting code which can correct bursts of errors. Later they developed multiple burst Array codes and presented decoding algorithim for the same. Abdel- Ghaffar, McEliece and Tilborg, (1988), defined burst identification codes which can be used to determine the pattern of errors and two dimensional correcting codes can be easily constructed by these codes. Zhang and Wolf (1988) developed a class of binary burst correcting quasi-cyclic codes. Blaum (1990) defined a family of efficient burst correcting array codes with better burst correction and performance and developed easy decoding algorithms. As data rates increase in communication systems, the burst error also increases accordingly.

Definition: A burst of length b is an n-vector in which the nonzero entries lie in b consecutive positions, the first and last of which are nonzero.

We now give some of the important results. The next two results are from Peterson and Weldon (1972) (refer Theorems 4.13 and 4.14).

(a) A linear code that has no burst of length b or less as a code word must have at least b parity-check symbols.

(b) For detecting all burst errors of length b or less with a linear block code of length n, b parity-check symbols are necessary and sufficient.

A lower bound on the number of parity checks required for a linear code that corrects all bursts of length b or less was found by Fire (1959) (c.f. theorem 4.16, Peterson and Weldon, 1972). The result is as follows:

The number of parity-check symbols in any linear block code over GF(q) that corrects all bursts of length b or less is at least

$$b-1 + \log_q[(q-1)\ (n-b+1)+1]$$

The following result analogous to the Varshamov-Gilbert-Sacks bound for the existence of a linear code that corrects all bursts of length b or less was obtained by Campopiano (c.f. Theorem 4.17, Peterson and Weldon, 1972).

There exists an (n, k) linear code that corrects any single burst of length $b < \frac{n}{2}$ or less for which the following inequality is satisfied

$$n-k \leq 2b + \log_q[(q-1)(n-2b-1) + 1]$$

There is another definition of a burst given by Chien and Tang (1965). This states that:

A burst of length b is a sequence of b digits, the first digit of which is nonzero.

This definition is found useful in convolutuional codes (refer Iwadare, 1967).

In this thesis a burst is to be taken of the former type only.

Wyner (1963) used the idea of associating weight with burst errors by constructing codes capable of correcting low-density bursts. Sharma and Dass (1974) studied in detail bursts with weight constraints by finding bounds on codes correcting/detecting bursts with various types of weight constraints.

1.8 Applications

1.8.1 Digital Techniques and Error-Control Coding

The number of communications and audio/video systems that treat voice or image signals as digital data, is rapidly increasing. One of the important characteristics of the *digital signals* is that these are more reliable in a noisy environment than analog signals. Since the detector for the digital data needs to decide only whether each signal is 0 or 1, digital symbols can often be detected perfectly, provided the noise is weak. However when the noise is not weak the detector may make an erroneous decision, i.e., it may decide that a symbol is 1 although it was originally 0 and vise-versa. But if the data are coded, i.e. some appropriate check symbols by annexing to the data symbols, the decoder can even correct or detect certain errors. Thus, when a signal is represented as digital data we make the signal detection more reliable by adding check symbols to the data symbols. This technique is called error control coding (for details refer, Imai, 1990). This technique has been widely used to digital communication and storage systems.

1.8.2 Communications System

Satellite Communication: In satellite communication the channel noise can be regarded as additive white Gaussian, thus the errors are mostly random. Since the transmitter power and the size of antennas of spacecraft are limited, it is desirable to use a code with large error correction capabilities to compensate for the low signal-noise ratio. This is because we can reduce the required transmitting power per bit ratio, to obtain a given bit-error rate by using an error correcting code. Self-orthogonal convolutional codes, which are decoded by a simple decoder, were mainly used for satellite communication. However, a ½ rate convolutional with Viterbi decoding which produces large error correction capabilities, is often used. High-rate BCH codes are also used in some cases.

Broadcasting: In teletext, which transmits digitised characters and figures overlapped with the TV signal, the most important type of error is the burst caused by the impulsive noise. Thus, a code with large error correcting capacity is required, but since the decoding is performed in the Television set itself, the decoder must be small. As a result, a different set cyclic code, which can be decoded by a relatively simple circuit, can be used.

Space Communication: Digital broadcasting systems are developed for the delivery of digital compressed video, audio and data services. The general requirements of such systems are high reliability and efficiency. Since digital television and broadcasting services channels are band limited, Trellis Coded Modulation (TCM) and Reed and Solomon Codes (RS) are considered usually for most of such applications.

Mobile Communication: Global System for Mobile Communication (GSM) is the digital cellular radio system. The GSM system provides speech, telefax, and data services such as telephony, paging, etc. To send message through the GSM system several types of signals need to be transmitted over the physical channel. To provide better efficiency, amplitude and accurate data transmission Channel coding of the speech data, channels coding of the signaling channels, and channel coding of the data channels, is being used. In the GSM system turbo codes are playing a very important role.

Code Division Multiple Access (CDMA) based digital cellular systems are distinguished from each other by a code rather than by frequency band allotted time slots. Cellular system allows access to resources by various techniques. The convolutional codes provide a good example of application in error protection in reverse CDMA channel as well as forward CDMA channel.

1.8.3 Computer System

In order to detect/correct errors in logic and arithmetic circuits of computers, codes based on partially check codes and Hamming codes are being used. However, codes especially suited to detect/correct errors in logic and arithmetic circuits are in the process of being developed.

Errors that occur in semiconductor memory systems can be regarded as random error or byte errors. The speed of the operations for semiconductor memories is very high, and therefore, the decoders must be extremely fast. Also the number of redundant symbols cannot be very large, as a result, a class of single error-correcting codes and double error-detecting Codes (SEC-DED) has been widely used for memory system. These codes are constructed on the basis of Hamming Codes, but the decoder for these codes is smaller and can be operated at a higher speed than that of Hamming codes. In some systems, single-byte error correcting and double byte error correcting codes (SbEC-DbEC) are used..

In most memory devices information is stored in two dimensions, and hence in such cases, error usually take the form of two-dimensional bursts. For example for the VLSI tam chips which are sensitive to alpha particle and other radiation effects, which can cause two-dimensional burst of errors, two-dimensional error-correcting codes can be used to combat such errors.

Magnetic Storage Device: In magnetic storage devices, to handle burst errors caused by defects of the device or due to dust, burst error correcting codes have been employed. Also Reed-Solomon like codes are found to be very useful. Fire codes are also being used, while (SbEC-DbEC) codes based on Reed-Solomon codes with interleaving are also used. In storage systems interleaved SbEC codes are being used.

Optical Disk System: In optical disk systems both random and burst errors occur and error rate of the device is relatively high, therefore, codes with large error correcting capabilities are required. As a result multiple coded Reed–Solomon code in conjunction with interleaving have been employed.

1.8.4 Audio-Video Systems

Since error-rate of devices is high and both random and burst errors occur in digital audio system, large error-correction capability is required. However, since the correlation between adjacent data is relatively high for audio signals, we can estimate the correct value of erroneous data by using the values of the data before and after the erroneous data. Miscorrection by the decoder causing a click noise must be strictly avoided, therefore, it desirable to stimulate the correct values of data that are likely to be miscorrected as described previously, instead of correcting any errors at the decoder. Doubly coded Reed-Solomon or cyclic codes with interleaving are used.

Requirement of error control codes for video systems are the same as those for audio systems, except that the probability of miscorrection does need not be as small as that for audio systems. And the processing speed must be much higher. Doubly coded Reed-Solomon or cyclic codes with interleaving are also used for video systems.

1.9 Problems Discussed in This Thesis

For a communication system to be reliable and efficient, the problem of choosing appropriate metric for a given channel is important, as the channel model should match the metric to be employed for developing suitable codes, for messages to be transmitted efficiently and reliably. Thus given a modulation scheme, one metric may be better suited than the other and such a choice is possible only if there is a way to design several metrics. Already there are two well-known metrics, one due to Hamming (1950) and other due to Lee (1958). Occasionally, references to some other metrics are also found in literature. However, there is no general method of generating metrics suitable to arbitrary channel. When metric used is that due to Hamming and the alphabet used for coding messages is non-binary, any digital change in one place is a single error, no matter what the magnitude of the change is. On the other hand, if metric used is that due to Lee, change of ± 1 in one place contributes one error, change of ±2 contributes weight of error as 2 and so on. In other words, the digital changes are '*too less*' distinguished in the case of Hamming metric, and '*too much*' in the case of Lee metric.

The present research work introduces a method of generating classes of metrics, each having larger number of metrics to choose one from, which may appropriately match a given channel.

In Chapter II the method of generating classes of metrics has been presented. Each metric is determined by a suitable partition, to be called P-*partition* of the alphabet set Z_q. A general member of this class of metrics is called a class-metric. Hamming and Lee metrics become particular rather than extremal class metrics. Some properties of codes in relation to minimum distances with reference to the new metrics and parity-check matrices have also been discussed. Finally, relationship between class-metrics and corresponding appropriate channels has been established.

Chapter III, contains the discussion of the problem of random error-correction by using class-metrics. It includes construction of single-class-error-correcting codes. The bounds have been derived on number of parity-checks required in codes which correct a given number of random class-errors and in codes which correct different types of class-error patterns, where the class-error patterns are obtained on the lines suggested, by Golomb (1969).

In situations, where channel introduces burst errors that have class-weight less (or greater) or equal to a pre-assigned number, the application of usual burst correcting codes reduces the efficiency of the communication system by using more parity checks than are sufficient to correct such errors. The problem of detection /correction of such burst errors needs to be considered separately.

Chapter IV considers problem of enumeration of such bursts and bounds on number of parity-checks required in codes correcting these bursts called burst with class-weight constraints.

Codes correcting bursts having length less than or equal to pre-assigned number and with/without class-weight constraint are not able to correct even a single random error, if it lies outside the bursts of given length.

Since this necessitated the study of the codes correcting random errors simultaneously with bursts with/without class-weight constraints. These types of codes are considered, wherein we obtained bounds on sufficient number of parity checks digits required in such codes, in Chapter V.

CHAPTER II

A Class of Metrics and their Properties

CHAPTER-II

A CLASS OF METRICS AND THEIR PROPERTIES

2.1 Introduction

The notion of metric (or a distance) plays a central role in coding theory, and the one, the almost universally used metric, is that due to Hamming (1950). Hamming Metric codes are ideal codes for balanced channels (Helstrom, 1961) in which probabilities of error for all symbols are equal. Another metric due to Lee (1958) is suitable for phase-modulation schemes, when phase-modulated signals are transmitted through additive gaussian noise. In chapter I, we have pointed out the limitations of those two metrics. There may be many channels and modulation schemes for which the Hamming or the Lee metric may not be quite suitable. This demands a search for other suitable metrics.

In the process of searching for new metrics, it is interesting to see that Hamming metric may be thought of as having arisen from the partition of the source alphabet in two distinct classes, one containing 0 (zero) and the other all the remaining letters of the alphabet. The nonzero elements have equal weight taken as one. A similar examination is possible for the Lee metric also. Some more details follow in section 2.3.

In the next section we explain a method of generating a class of metrics by suitably partitioning the alphabet set. Any general member of this class of metrics is called a *class-metric,* whereas the partition determining it will be called a *$\mathcal{P}$-partition.* In Section 2.3, we show that

Hamming and Lee metrics are special class-metrics. Some algebraic studies of $\mathcal{P}$-partitions are taken up in section 2.4.

2.2 Definition of the New Metric

We consider n-vectors over the ring $Z_q=\{0,1, \ldots q-1\}$, the integers mod q. The class of metrics that we introduce depends on a scheme of partitioning Z_q. Each partition gives rise to a new metric. Some conditions are required over the partitions that we consider. These conditions are required essentially to make the distance defined, to be bonafide metric in the space of n-tuples over Z_q. To be specific and precise, we define a partition $\mathcal{P}$ suiting our purpose as follows:

$\mathcal{P}$-partition: Let us consider a partition of Z_q into (disjoint, non-empty) subsets $B_0, B_1, \ldots B_{m-1}$, where m is an integer greater that or equal to 2, such that

than

i) $B_0=\{0\}$ and for $i \in Z_q$; $i \in B_s \Leftrightarrow q-i \in B_s$,

ii) If $i \in B_s$, $j \in B_t$ and $s > t$, then[1],
$\min\{i, q-i\} > \min\{j, q-j\}$,

and

[1] > is taken in arithmetical sense.

iii) If $s \geq t$, $|B_s| \geq |B_t|$ except for $s=m-1$,

in which case we should have $\left|B_{m-1}\right| > \frac{1}{2}\left|B_{m-2}\right|$, where

$|B|$ = number of elements in B.

In all our studies that follow a partition of Z_q satisfying the above conditions will be called **$\mathcal{P}$-partition**.

Next we come to the definition of weight and distance depending on $\mathcal{P}$-partition.

Weight of an Integer with respect to a $\mathcal{P}$-partition: The weight of an element j belonging to Z_q corresponding to a $\mathcal{P}$-partition $\mathcal{P}_1=\{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, which will be termed as *class-weight* of j and denoted by $w_{\mathcal{P}_1}(j)$, is defined as the index of the class to which j belongs in $\mathcal{P}_1$, i.e.,

If $j \in B_s$ then $w_{\mathcal{P}_1}(j) = s$, $0 \leq s \leq m-1$.

The term class-weight has been coined for the new weight of an element of Z_q corresponding to a $\mathcal{P}$-partition $\mathcal{P}_1$, because the element takes the weight of the class to which it belongs in $\mathcal{P}_1$.

Class-Weight of a Vector: The class-weight $w_{\mathcal{P}_1}(\underline{u})$ of an n-tuple $\underline{u} = (a_1, a_2, \ldots, a_n)$, $a_i \in Z_q$, corresponding to $\mathcal{P}$-partition $\mathcal{P}_1$, is defined as the sum of the class-weights of its components, i.e.,

$$w_{\mathcal{P}_1}(\underline{u}) = \sum_{i=1}^{n} w_{\mathcal{P}_1}(a_i) \qquad \text{... (eq 2.1)}$$

Class-Distance of a $\mathcal{P}$-partition: For a given $\mathcal{P}$-partition $\mathcal{P}_1$, the class-distance between two elements a and b of Z_q , can be defined in terms of the notion of class weight. Given two elements a, b $\in Z_q$, the *class-distance* $d_{\mathcal{P}_1}(a, b)$, between a and b for a $\mathcal{P}$-partition $\mathcal{P}_1$ is given by

$$d_{\mathcal{P}_1}(a, b) = w_{\mathcal{P}_1}(a - b)$$

Next, given two n-tuples $\underline{u} = (a_1, a_2, \ldots , a_n)$, and $\underline{v} = (b_1, b_2, \ldots , b_n)$, where $a_i, b_i \in Z_q$, the *class-distance between vectors $\underline{u}$ and $\underline{v}$ associated with $\mathcal{P}_1$* is defined as the sum of the class-distances between their components, i.e.,

$$d_{\mathcal{P}_1}(\underline{u}, \underline{v}) = \sum_{i=1}^{n} d_{\mathcal{P}_1}(a_i, b_i) \qquad \text{... (eq 2.2)}$$

It may be observed that

$$d_{\mathcal{P}_1}(\underline{u}, \underline{v}) = w_{\mathcal{P}_1}(\underline{u} - \underline{v}) = \sum_{i=1}^{n} w_{\mathcal{P}_1}(a_i - b_i) \qquad \text{... (eq 2.3)}$$

In this thesis, $w_{\mathcal{P}_1}(x)$ and $w_{\mathcal{P}_1}(\underline{u})$ will denote class-weights of an element x of Z_q and an n-tuple $\underline{u}$ respectively over Z_q corresponding to a $\mathcal{P}$-partition $\mathcal{P}_1$ of Z_q. Similarly, $d_{\mathcal{P}_1}(x, y)$ and $d_{\mathcal{P}_1}(\underline{u}, \underline{v})$ denote respectively distances between two elements of Z_q and two n-tuples over Z_q corresponding to $\mathcal{P}$-partition $\mathcal{P}_1$.

The distance $d_{\mathcal{P}_1}(\underline{u}, \underline{v})$ so defined, introduces a metric over z_q^n, the space of n-tuples over Z_q. This will be established after giving an example and some explanations of the new ideas.

Example:

Let $Z_q = \{0,1, \dots , 12\}$, $q = 13$. Consider a $\mathcal{P}$-partition of Z_{13} given by

$$\mathcal{P}_1 = \{B_0, B_1, B_2, B_3\},$$

such

$B_0 = \{0\}$, $B_1 = \{1,12\}$, $B_2 = \{2,3,4,9,10,11\}$ and $B_3 = \{5,6,7,8\}$; then according to our definitions:

$$w_{\mathcal{P}_1}(0) = 0, \qquad w_{\mathcal{P}_1}(1) = 1`, \qquad w_{\mathcal{P}_1}(12) = 1, \qquad w_{\mathcal{P}_1}(4) = 2, \qquad w_{\mathcal{P}_1}(7) = 3$$

Also, if $\underline{u} = (2,8,12,6,5)$ and $\underline{v} = (6,2,1,6,10)$,

then $\underline{u}$-$\underline{v} = (9,6,11,0,8)$ and

$$d_{\mathcal{P}_1}(\underline{u}, \underline{v}) = w_{\mathcal{P}_1}(\underline{u} - \underline{v}) = w_{\mathcal{P}_1}(9) + w_{\mathcal{P}_1}(6) + w_{\mathcal{P}_1}(11) + w_{\mathcal{P}_1}(0) + w_{\mathcal{P}_1}(8)$$

$$= 10$$

An explanation of the new idea

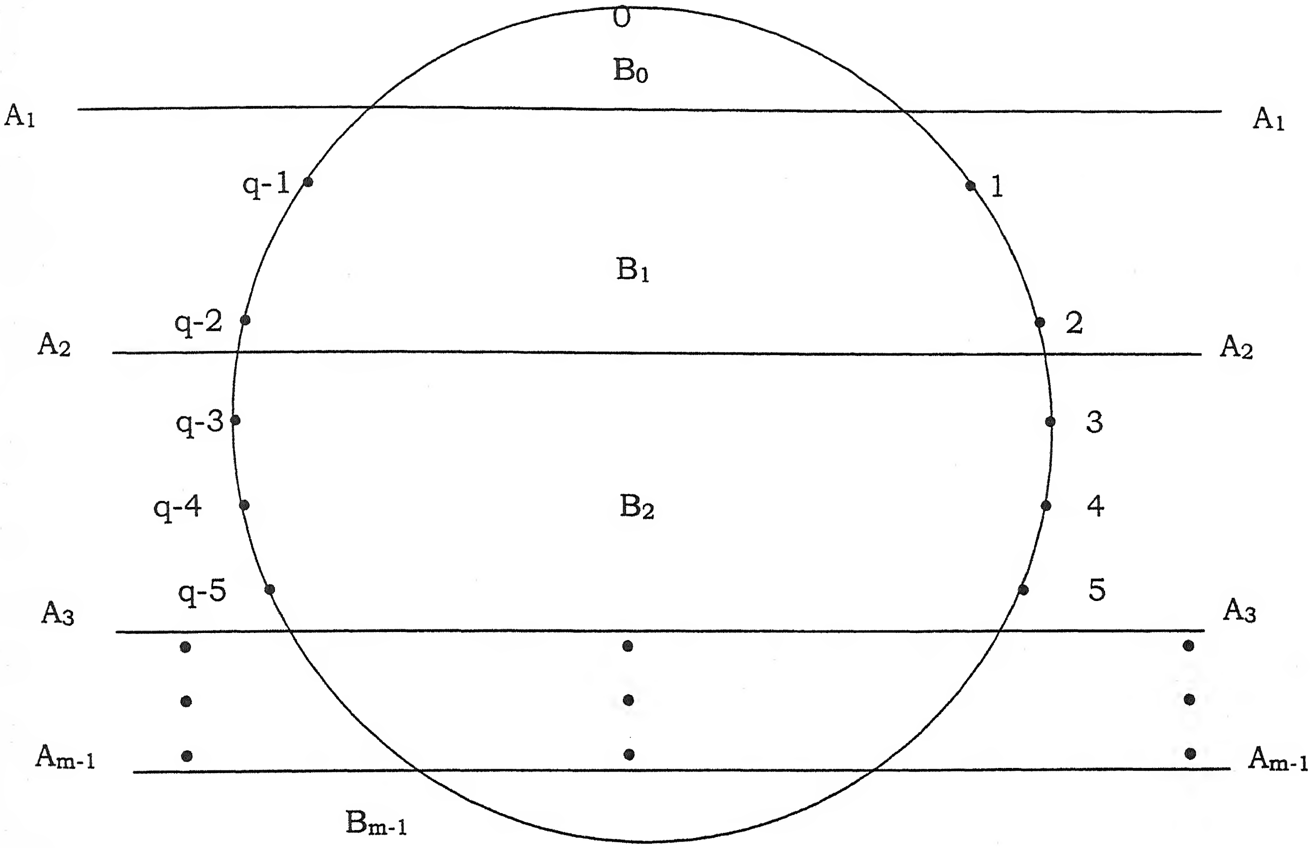


Figure 2.1 Schematic Representation of a $\mathcal{P}$-Partition of Z_q

Let the alphabet set Z_q be represented by a circle with integers 0,1,...,q-1 being points equally spaced on its circumference as shown in Fig. 2.1. Then a $\mathcal{P}$-partition of Z_q may be considered as the partition of the circle by the parallels A_iA_i(i=1, ..., m-1) which are all taken perpendicular to the diameter thorough 0 with the classes B_i, i=2, ..., m-2, being given by points lying on sections of the circle between parallel lines A_iA_i and $A_{i+1}A_{i+1}$ and classes B_0 and B_{m-1} are given by respectively point lying above A_1A_1 and points lying below $A_{m-1}A_{m-1}$. The conditions for $\mathcal{P}$-partition given above require that distance between successive pairs of lines A_1A_1, A_2A_2, ... , $A_{m-1}A_{m-1}$, goes on increasing and the length of the arc below $A_{m-1}A_{m-1}$ is not less than one of the two arcs between $A_{m-2}A_{m-2}$ and $A_{m-1}A_{m-1}$. The points between A_iA_i and $A_{i+1}A_{i+1}$ have class-weight i.

The 0, which is above A_1A_1, has class-weight zero and the points below $A_{m-1}A_{m-1}$ have class-weight (m-1).

It can be easily seen that the class-distance $d_{\mathcal{P}_1}$ is a bonafide metric on Z_q^n, the set of all n-tuples over Z_q. In other words, it can easily be established that for $\underline{u}$, $\underline{v}$ and $\underline{w} \in Z_q^n$

i) $d_{\mathcal{P}_1}(\underline{u}, \underline{v}) \geq 0$ and $d_{\mathcal{P}_1}(\underline{u}, \underline{v}) = 0$, if $\underline{u} = \underline{v}$,

ii) $d_{\mathcal{P}_1}$ is symmetric in Z_q^n, i.e., $d_{\mathcal{P}_1}(\underline{u}, \underline{v}) = d_{\mathcal{P}_1}(\underline{v}, \underline{u})$

and

iii) $d_{\mathcal{P}_1}$ satisfies the triangular inequality in Z_q^n viz.,

$$d_{\mathcal{P}_1}(\underline{u}, \underline{v}) \le d_{\mathcal{P}_1}(\underline{u}, \underline{w}) + d_{\mathcal{P}_1}(\underline{w}, \underline{v})$$

2.3 Hamming and Lee Metrics as Special Class-metrics

Now we show that our metric generalises the Hamming and Lee metrics.

Consider a $\mathcal{P}$-partition $\mathcal{P}_H = \{\{0\}, \{1,2, \dots , q-1\}\}$ of Z_q. Let us denote the Hamming weight of an element x of Z_q by $w_H(x)$.

Then $w_{\mathcal{P}_H}(0) = 0 = w_H(0)$ and $w_{\mathcal{P}_H}(i) = 1 = w_H(i)$ for $i \in Z_q \sim \{0\}$.

Therefore

$$w_{\mathcal{P}_H}(x) = w_H(x) \quad \text{for } x \in Z_q \qquad \dots \text{(eq 2.4)}$$

Further, for an n-tuple $\underline{u} = (a_1, \dots, a_n)$ over Z_q, using (eq 2.2) and (eq 2.4), we easily have

$$w_{\mathcal{P}_H}(\underline{u}) = \sum_{i=1}^{n} w_{\mathcal{P}_H}(a_i) = \sum_{i=1}^{n} w_H(a_i) = w_H(\underline{u}) \qquad \dots \text{(eq 2.5)}$$

Hence class-weight of an n-tuple over Z_q, corresponding to $\mathcal{P}_H$ is equal to its Hamming weight.

Also from (eq 2.3) and (eq 2.5) it follows that class-distance $d_{\mathcal{P}_H}(\underline{u}, \underline{v})$ between two n-tuples $\underline{u}$ and $\underline{v}$ is equal to the Hamming distance

$d_H(\underline{u}, \underline{v})$ between them.

Again consider a $\mathcal{P}$-partition $\mathcal{P}_L$ of Z_q, given by

$$\mathcal{P}_L = \{B_0, B_1, \dots , B_{[q/2]}\},$$

Where $B_i = \{i, q-i\}$ for $i = 1, \dots, \lfloor q-2 \rfloor$

It is easy to see that

$$w_{\mathcal{P}_L}(x) = w_L(x) \quad \text{for } x \in Z_q,$$

where $w_L(x)$ denotes that Lee-weight of the element x of Z_q.

Also using arguments similar to those used for the case of the partition $\mathcal{P}_H$, it may be shown that $w_{\mathcal{P}_L}(\underline{u})$, the class-weight of an n-tuple $\underline{u}$ over Z_q is equal to its Lee-weight $W_L(\underline{u})$ and further that the class-distance $d_{\mathcal{P}_L}(\underline{u}, \underline{v})$ between two n-tuples $\underline{u}$ and $\underline{v}$, corresponding to P_L equals $d_L(\underline{u}, \underline{v})$, the Lee-distance between the two n-tuple $\underline{u}$ and $\underline{v}$.

To facilitate further references, we record our discussions given above in the form of a theorem given below:

Theorem 2.1: Given the space of n-tuple over Z_q the integers mod q; $d_{\mathcal{P}_1}$ the class-metric defined earlier coincides with

i) Hamming metric if $\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\}$,

Where $B_1 = \{1,2, \ldots, q-1\}$ and

ii) Lee metric if $\mathcal{P}_1 = \mathcal{P}_L = \{B_0, B_1, \ldots, B_{m-1}\}$

Where $m = \lfloor (q+2)/2 \rfloor$ and $B_i = \{i, q-i\}$, $i=1,2, \ldots, m-1$.

In our study, we will be using d_H (or simply d) and d_L respectively instead of $d_{\mathcal{P}_H}$ and $d_{\mathcal{P}_L}$.

2.4 Results of codes with a given minimum Class-distance

In the previous chapter we have emphasised the importance of minimum distance of a code for correcting additive random errors. The concept of minimum distance for a code can be extended to class-distance on the lines parallel to those for Hamming and Lee metrics. Formally we may put it as follows:

Definition: Given a code $\mathcal{C}$ over Z_q, the ring of integers mod q and a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, the *minimum class-distance* of the code $\mathcal{C}$ is the minimum of all the class-distances between pairs of distinct code words. It will be denoted by $d_{\mathcal{P}_1}(\mathcal{C})$ or $d_{\mathcal{P}_1}$.

In the case of the partitions $\mathcal{P}_H$ and $\mathcal{P}_L$ leading respectively to the Hamming and Lee metrics we shall shorten $d_{\mathcal{P}_H}$ and $d_{\mathcal{P}_L}$ to d_H and d_L respectively. Thus $d_H(\mathcal{C})$ or d_H will denote the minimum Hamming distance of a code and similarly $d_L(\mathcal{C})$ or d_L will denote the minimum Lee distance of a code $\mathcal{C}$.

Also, the minimum class-weight of a code is the smallest in the set of all class-weights of nonzero code words of the given code $\mathcal{C}$.

It is easy to see that, the minimum class-distance and minimum class-weight coincide for a linear code.

A result which provides bounds on $d_{\mathcal{P}_1}$, the minimum class-distance of a linear code $\mathcal{C}$, in terms of minimum Hamming distance d_H and the minimum Lee–distance d_L of the code $\mathcal{C}$ may now be given, it is stated below, the proof of which follows easily.

Theorem 2.2: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, q prime and a linear code $\mathcal{C}$ over Z_q having d_H and d_L and $d_{\mathcal{P}_1}$ respectively as minimum Hamming distance, minimum Lee distance and the minimum class-distance of $\mathcal{C}$ determined by $\mathcal{P}_1$, then

$$d_H \leq d_{\mathcal{P}_1} \leq \min\left\{\left\lfloor \frac{w(\mathcal{P}_1)d_H}{q-1} \right\rfloor, d_L\right\} \qquad \ldots \text{(eq 2.6)}$$

Where $w(\mathcal{P}_1)$ denotes the sum of the class-weights of the letters of the alphabet (0,1, ..., q-1}, i.e.,

$$W(\mathcal{P}_1) = \sum_{i=1}^{m-1} i\left|B_i\right| \qquad \text{... (eq 2.7)}$$

Remarks: Simple consequences of this result for partitions leading to Hamming and Lee metrics are rather straight and may be recorded as follows :

In the case of Hamming metric:

$$W(\mathcal{P}_1) = q - 1 \qquad \text{... (eq 2.8)}$$

and therefore, the inequality (eq 2.6) takes the obvious form

$$d_H \leq d_H \leq d_H, \qquad \text{as } d_H = \min\{d_H, d_L\}$$

Further, in the case of Lee metric, for q an odd prime, we have $\mathcal{P}_L = \left\{B_0, B_1, \ldots, B_{(q-1)/2}\right\}$, $B_i = \{i, q - i\}$ for i = 1,2,....,(q-1)/2.

Therefore

$$W(\mathcal{P}_L) = \sum_{i=1}^{(q-1)/2} i\left|B_i\right| = \sum_{i=1}^{(q-1)/2} i.2 = (q^2 - 1)/4 \qquad \text{... (eq 2.9)}$$

and hence form (eq 2. 6), we get

$$d_H \le d_L \le \left\lfloor \frac{q^2-1}{4}\,\frac{1}{q-1}\,d_H \right\rfloor = \left\lfloor \frac{q+1}{4}\,d_H \right\rfloor$$

or

$$d_H \le d_L \le \left\lfloor \frac{q+1}{4}\,d_H \right\rfloor, \qquad \text{... (eq 2.10)}$$

which gives a better upper bound on d_L as compared to the bound given by two inequalities

$$d_H \le d_L \le \lfloor q/2 \rfloor\, d_H,$$

due to Chiang and Wolf (1971, Inequality (8)).

Definition: The *class-weight of an m×n matrix A* over Z_q corresponding to the $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q is the sum of class-weights of the m rows, each row being taken as an n-vector over Z_q, or equivalently, as the sum of the class-weights of the n columns, each column being taken as an m-vector over Z_q.

It is easy to see that the class-weight of an m×n matrix A= (a_{ij}) is given by

$$\sum_{i=1}^{m}\sum_{j=1}^{n} w_{\mathcal{P}_1}(a_{ij})$$

The study of linear error-correcting codes, their constructions, error-correcting capabilities and decoding algorithms etc., is facilitated with the use of parity-check matrices. Next theorem, a simple consequence of Theorem 2.2 finds a relation between minimum class-weight of a code and the number of linearly independent columns of its parity-check matrix.

Theorem 2.3: For a given $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, \ldots, B_{m-1}\}$ of Z_q, q prime, determining the class-weight under consideration, a linear code $\mathcal{C}$ that is the null space of a matrix H has minimum class-weight w implies that every combination of $\frac{(q-1)w}{w(\mathcal{P}_1)} - 1$or fewer columns of H is linear independent.

Proof: The minimum class-weight of the linear code is w. therefore from Theorem 2.2 we have

$$w \leq \frac{w(\mathcal{P}_1)}{q-1} d_H$$

where $W(\mathcal{P}_1)$denotes the sum of the class-weights of letters of the alphabet set {0,1, ..., q-1} and d_H is the minimum Hamming weight of $\mathcal{C}$.

The result follows form the fact that for a linear code with a minimum Hamming distance d_H, any d_{H-1} or less columns of H should be linearly independent.

The result of Theorem 2.3 is further refined in Theorem 2.4 through the introduction of a new concept, a modification of the idea of linear dependence, suitable for class-metric codes.

Definition: A Linear combination

$$\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 + \cdots + \lambda_n \underline{u}_n$$

of vectors $\underline{u}_1$, $\underline{u}_2$, ..., $\underline{u}_n$, for $\lambda_i \in Z_q \sim \{0\}$ will be called a *linear combination of class-weight w* if the vector (λ_1, ..., λ_n) has class-weight w, corresponding to a $\mathcal{P}$-partition $\mathcal{P}_1$.

Theorem 2.4: For a given $\mathcal{P}$-partition $\mathcal{P}_1$ = {B_0, B_1, ..., B_{m-1}} of Z_q determining the class-weight under consideration, an (n, k) linear code $\mathcal{C}$, with H as its parity-check matrix, has minimum class-weight at least w if and only if every linear combination of class-weight w-1 or less of columns from amongst the columns of H, is non-null.

Proof: Let H = [C_1, ..., C_n] be the parity–check matrix of the code $\mathcal{C}$, where C_i, an (n-k)-vector, denotes the i^th^ column of H. For any non-null vector $\underline{u}$ =(a_1, ..., a_n) over Z_q,

$$\underline{u}H^T = a_{i_1} C_{i_1} + \ldots + a_{i_k} C_{i_k} \quad (\text{with } a_{i_k} \neq 0) \qquad \ldots \text{(eq 2.11)}$$

is a linear combination of class-weight $w_{\mathcal{P}_1}(\underline{u})$ of columns form amongst the columns of H.

Now if every linear combination of class-weight w-1 or less of columns form amongst the columns of H is non-null then for an n-tuple

$\underline{u}$ = (a_1, ..., a_n) with class-weight $w_{\mathcal{P}_1}(\underline{u})$ less than or equal to w-1, we have

$$\underline{u}\, H^T \neq 0 \qquad \text{(using eq 2.11)}$$

Hence $\underline{u}$ is not a code word in $\mathcal{C}$. therefore no n-tuple with class-weight w-1 or less can be a code word in $\mathcal{C}$. From this it follows that every code word in $\mathcal{C}$ must have class-weight at least w.

Conversely, let the minimum class-weight of the code $\mathcal{C}$ be w and

$$a_{i_1} C_{i_1} + a_{i_2} C_{i_2} + \dots + a_{i_t} C_{i_t}, \qquad \text{... (eq 2.12)}$$

$a_{ij} \neq 0 \; 1 \leq i_j \leq n,$

be a linear combination of class-weight not exceeding w-1 of column from those of H. Clearly

$$\sum_{j=1}^{t} w_{\mathcal{P}_1}(a_{i_j}) \leq w - 1 \qquad \text{... (eq 2.13)}$$

consider an n-vector $\underline{u}$= (u_1, ..., u_n) such that

$$u_{i_j} = a_{i_j} \qquad \text{for } j = 1, \dots, t.$$

with rest of the entries in $\underline{u}$ being 0, then

$$w_{\mathcal{P}_1}(\underline{u}) = \sum_{j=1}^{t} w_{\mathcal{P}_1}(a_{i_j}) \le w - 1 \qquad \text{(from (eq 2.13)} \qquad \text{... (eq 2.14)}$$

As minimum class-weight of $\mathcal{C}$ is w, therefore, $\underline{u}$ cannot be a code word in $\mathcal{C}$. Hence

$$\underline{u}\,H^T \ne 0,$$

which implies

$$a_{i_1} C_{i_1} + a_{i_2} C_{i_2} + \ldots + a_{i_t} C_{i_t} \ne \underline{0}$$

This completes the proof of the theorem.

Corollary 2.1: In the case of Hamming metric, the phrase every linear combination of class-weight w-1 or less of columns form those of H is non-null occurring the Theorem 2.4 is equivalent to the phrase every combination of w-1 or fewer columns of H is linearly independent and hence the result of Theorem 2.4 reduces to that of Corollary 3.1 of Peterson and Weldon (1972).

2.5 Channel Models and Class-Metrics

In this section, we characterized a *discrete, memoryless* and *symmetric channel* for class-metric.

We consider only those matchings of a channel and a metric $d_{\mathcal{P}_1}$ for which the input alphabet and the output alphabet each equals the ring

Z_q of integers mod q and the set $\{p(j \mid i)\}$ of probabilities of receiving j's when i's are transmitted, satisfies

i) $p(j \mid i = p(j-i \mid 0) = p(j-i)$ for $i, j \in Z_q$

and

ii) p(b), the probability of receiving b when 0 is transmitted, depends on the class B_s to which b belongs in $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the metric $d_{\mathcal{P}_1}$ in Z_q^n. Let

$$p(b) = p_s \text{ for } b \in B_s$$

Then we call $\{p_s\}_{s=1}^{m-1}$, the set of class–error probabilities of the channel.

The next two theorems characterize channels in terms of class-error probabilities determined buy a class-metric.

Theorem 2.5: A discrete, memoryless symmetric channel, having input symbols form Z_q strictly matches a class-metric $d_{\mathcal{P}_1}$ determined by the $\mathcal{P}$-partition

$\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q; for MLD iff

$$p_0 > p_1 \qquad \text{and} \qquad p_i = \frac{p_1^i}{p_0^{i-1}}$$

Theorem 2.6: A discrete, memoryless, symmetric channel is strictly matched to the class-metric $d_{\mathcal{P}_1}$ determined by the $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q; for BDD of radius t, iff

$$\prod_{\substack{\sum_{j=1}^{m-1} jn_j \le t \\ \sum_{j=0}^{m-1} n_j = n}} p_j^{n_j} > \prod_{\substack{\sum_{j=1}^{m-1} jn_j \ge t+1 \\ \sum_{j=0}^{m-1} n_j = n}} p_j^{n_j}$$

CHAPTER III

CONSTRUCTION OF CLASS-ERROR-CORRECTING CODES AND BOUNDS ON NUMBER OF PARITY-CHECKS

3.1 Introduction

3.2 Codes Correcting Patterns of Class-Weight One

3.3 Hamming-Type and Plotkin-Type Bounds

3.4 Varshamov-Gilbert-Like Bound

3.5 Codes Detecting/Correcting Random Errors Having Constraint on Magnitude of Error in a Position and/or Number of Error Positions

CHAPTER-III

CONSTRUCTION OF CLASS-ERROR-CORRECTING CODES AND BOUNDS ON NUMBER OF PARITY-CHECKS

3.1 Introduction

As emphasized earlier, a good part of coding theory is devoted to the construction of codes detecting/correcting errors and finding out of decoding algorithms for such codes. Most of the codes have been constructed to correct errors arising out of the channels matching Hamming metric. Though, there are some good Lee-metric codes also (refer Berlekamp, 1968; Golomb and Welch, 1968; Chiang and Wolf, 1971).

Chapter III is devoted to the construction of some codes correcting additive errors on symmetric memoryless channels matching a metric not necessarily that due to Hamming or Lee, but a class-metric as introduced in previous chapter. Also we find out bounds on number of parity checks required in codes correcting error patterns on these channels.

In Section 3.2 we give single-class-error-correcting codes by constructing their parity-check matrices using two different methods. The construction of the parity-check matrices is on the lines of those given for Hamming codes. (refer Peterson and Weldon, 1972) or codes correcting single Lee-errors (refer Berlekamp, 1968). An example is given to demonstrate the advantage of this general procedure.

Section 3.3 derives Hamming-sphere-type and Plotkin-type bounds for codes correcting a given number of class-errors. To derive these bounds, we extend the notions of a sphere, surface area and volume of a sphere (refer Berlekamp, 1968), already defined for Hamming and Lee metrics, to those for a general class-metric. Also, for the sake of convenience of notation, we introduce the notion of a spherical hull.

In Section 3.4 we find Varshamov-Gilbert-type bounds on sufficient number of parity-checks for codes correcting a given number of class-errors.

In Section 3.5, we introduce a number of error-spheres on the lines suggested by Golomb (1969) and make use of these error-spheres in fining out necessary and sufficient number of parity checks required in codes correcting different type of error patterns.

We start by defining an error pattern of a given class-weight.

Definition: Let $\underline{v} = (b_1, \ldots, b_n)$ be the received vector when $\underline{u} = (a_1, \ldots, a_n)$ was transmitted, then the vector $\underline{e} = (e_1, \ldots, e_n)$ with the code $\underline{e}_i = b_i\text{-}a_i$, will be called an error pattern of class-weight t if the class-weight of the vector $\underline{e}$ is t.

In particular a vector $\underline{e} = (0, 0, ..., 0, e_j, 0, ..., 0)$ is an error pattern of class-weight one, where the element e_j of Z_q has class-weight one.

The codes considered in this chapter are over the finite field Z_q of integers mod q, for q prime. Also the class-metric to be employed in these codes is determined by the $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q.

3.2 Codes Correcting Patterns of Class-Weight One

We detail the procedure for the construction and decoding of the codes capable of correcting all error patterns of class-weight one. The following definition will be useful in describing the decoding procedures for these codes:

Definition: The norm of a r-column-vector $\underline{u}^T = (a_1, \ldots, a_r)^T$, a_i belonging to Z_q, denoted by $\|\underline{u}^T\|$, is defined as

$$\|\underline{u}^T\| = \|(a_1, \ldots, a_r)^T\| = a_1 q^{r-1} + \ldots + a_{r-1} q + a_r \qquad \ldots \text{(eq 3.1)}$$

It is straight forward to show that

$$\|\underline{u}^T\| = \|\underline{v}^T\| \Leftrightarrow \underline{u}^T = \underline{v}^T .$$

Construction: A code is fully devised if we are able to construct a parity check matrix H for it. Also, a code capable of correcting error patterns of class-weight one should have minimum *class-weight at least three.*

Therefore, from Theorem 2.4, it follows that every linear combination of class-weight two or less of the columns of H should be non-null. This fact (c.f. Peterson and Weldon, 1972) can help us in the construction of a suitable parity-check matrix H for the code.

Let a nonzero r-tuple say C_1 over Z_q be taken as the first column of H. In general, after selecting j-1 columns $C_1, \ldots, C_{j-1}$ of H, a nonzero r-tuple is taken as j^{th} column C_j of H, provided that a linear combination of class-weight less than or equal to two, of any of the previous column and C_j is non-null, i.e.,

$$\begin{array}{ll} & \left.\begin{array}{l} aC_t + bC_j \neq 0, \\ 1 \leq t \leq j-1 \text{ and } w_{\mathcal{P}_1}(a) + w_{\mathcal{P}_1}(b) \leq 2 \end{array}\right\} \\ \textit{where} & \end{array} \qquad \ldots \text{(eq 3.2)}$$

Choosing n columns of H in this way, we are able to construct a parity-check matrix of a single class-error-correcting code of length n.

The largest value of n, i.e., a maximum length code with a pre-assigned number of parity checks r will be given by a parity-check matrix H having maximum number of columns that we can select in this fashion. Let n_{max} denote the maximum value of n, the length of the code constructed above having r parity checks. Next we determine upper and lower bounds of n_{max} in the next theorem.

Theorem 3.1: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration; bound over n_{max}, the maximum possible length of the single class-error-correcting code having r parity checks, constructed above, are given by

$$\left(\frac{q^r-1}{q-1}\right)\left\lceil\frac{q-1}{\left|B_1B_1^{-1}\right|}\right\rceil \le n_{\max} \le \left(\frac{q^r-1}{q-1}\right)\left\lfloor\frac{q-1}{\left|B_1\right|}\right\rfloor \qquad \text{... (eq 3.3)}$$

Where $\lceil x \rceil$ and $\lfloor x \rfloor$ denote respectively the smallest integer containing x and the largest integer contained in x and

$$B_1B_1^{-1} = \{b_1b_2^{-1} : b_1, b_2 \in B_1\}$$

and

$\left|B_1\ B_1^{-1}\right|$ = number of elements in $B_1B_1^{-1}$.

Proof: We prove the result by taking $n_{\max}$ as the maximum possible number of columns in the parity-check matrix H of the given code.

From the argument given in the construction of the code and from (eq 3.2), it follows that it is sufficient to find out the maximum number of r-tuples over Z_q, for which B_1-multiples (i.e., multiples by elements of B_1) of one r-tuple, are different from B_1-multiples of the other r-tuple, i.e., if C_t and C_j are two such r-tuples, then

$$aC_t \ne bC_j \qquad \text{for } a, b \in B_1 \qquad \text{... (eq 3.4)}$$

(for a $\in B_1 \Leftrightarrow -a \in B_1$)

For this, we consider the set of all nonzero r-tuples. This set has q^r-1 elements. We partition this set into $(q^r-1)/(q-1)$ classes; each class containing q-1 mutual scalar multiple r-tuple. From the construction of the classes, it is clear that an r-tuple from one class cannot be a scalar multiple of an r-tuple from another class. Therefore, an r-tuple from one class cannot be a B_1-multiple (because B_1 is a subset of $Z_q \sim \{0\}$) of an r-tuple from another class.

Thus, there are as least $(q^r-1)/(q-1)$ r-tuples, one from each class, such that B_1-multiples of one r-tuple are distinct from B_1-multiples of the other r-tuple.

Further, if l is the maximum possible number of those elements of $Z_q \sim \{0\}$, for which B_1-multiples of one element are distinct from B_1-multiples of the other elements, then we can choose maximum l r-tuples from each class of the partition of the set of all r-tuples. Therefore,

$$n_{\max} = l\left(\frac{q^r-1}{q-1}\right) \qquad \text{... (eq 3.5)}$$

In view of (eq 3.5), it is sufficient to find bounds on l, in order of prove (eq 3.3)

Obviously,

$$l \le \left\lfloor \frac{q-1}{\left|B_1\right|} \right\rfloor \qquad \text{... (eq 3.6)}$$

Further, it is easy to see that $l \geq 1$; as any element of $Z_q \sim \{0\}$ can be chosen as the first element in order to find the lower bound of l. Let us take this element as $\alpha_1=1$.

Again, a nonzero element α_2 exists in Z_q such that no B_1-multiple of α_2 equals an element of B_1, i.e.,

$$\alpha_2 B_1^* \cap B_1 = \phi \qquad \text{... (eq 3.7)}$$

If and only if

$$\alpha_2 \notin B_1 B_1^{-1}.$$

Therefore, it follows that

$$l \geq 2, \ \text{ if } (q-1) > \left|B_1 B_1^{-1}\right| \qquad \text{... (eq 3.8)}$$

[*] $(\alpha\beta = \{\alpha b : b \in B)$

Continuing like this, we can find out nonzero elements $\alpha_1=1, \alpha_2, \ldots, \alpha_f$ in Z_q such that B_1-multiples of one of α's the are distinct from B_1-multiples of the other α, if and only if

$$\alpha_j \notin \alpha_i B_1 B_1^{-1} \qquad \text{for } j > i$$

At worst all the sets $B_1 B_1^{-1}, \alpha_2 B_1 B_1^{-1}, \ldots, \alpha_{f-1} B_1 B_1^{-1}$ may be disjoint. Therefore, we can find out an α_f if

$$(q-1) > (f-1)\left|B_1 B_1^{-1}\right| \qquad \ldots \text{(eq 3.9)}$$

As l is the maximum value for f, therefore

$$(q-1) \not> l\left|B_1 B_1^{-1}\right|,$$

i.e.,

$$\left\lceil \frac{(q-1)}{\left|B_1 B_1^{-1}\right|} \right\rceil \leq l \qquad \ldots \text{(eq 3.10)}$$

From (eq 3.5, eq 3.6 and eq 3.10) we get the required bounds of n_{max} .

Now we describe a decoding procedure for the code constructed in this section.

Decoding of the above Code: To facilitate decoding of the code, we arrange the columns in H in the order of increasing norms of the columns, i.e., if $\underline{u}^T$ and $\underline{v}^T$ are two r-columns in H then $\underline{u}^T$ precedes $\underline{v}^T$ in H if $\|\underline{u}^T\|$, the norm of $\underline{u}^T$ is less than $\|\underline{v}^T\|$, the norm of $\underline{v}^T$. After arranging the columns in H in this manner, we denote by $p_n(\underline{u}^T)$ the number of the position of columns $\underline{u}^T$ in H.

Let $\underline{b}$ be the received n-vector when an n-vector $\underline{a}$ was transmitted such that class-distance between $\underline{b}$ and $\underline{a}$ is one or less, i.e., class-weight of the error-pattern $\underline{e}$ added to the transmitted vector does not exceed one. We calculate the syndrome $\underline{b}H^T$ of the received vector $\underline{b}$. If this syndrome is the null vector, then $\underline{b}$ is a code word and we assume that $\underline{b}$ is the transmitted code word. On the other hand, if the syndrome of the received vector is non-null, we know that, it is equal to the syndrome of the error-pattern. Also, an error-pattern of class-weight one has only one non-zero component. Therefore, syndrome of such an error-pattern is a multiple of a column of H with an element of the class B_1 .

Thus the syndrome of the received vector is a multiple of a column of H with an element of B_1. By the construction of H, multiples of the columns of H by elements of B_1 are all distinct. Let.

$$\underline{b}H^T = f.C_j,$$

Where f is an element of B_1 and C_j is a column in H. Then f is the error in $p_n(C_j)$th position. Thus, error pattern $\underline{e}$ is an n-vector in which $p_n(C_j)$th component is f and all other components are zero. Subtracting $\underline{e}$ from the received vector $\underline{b}$ we get the required vector.

An example is given below to show that if the error patterns on a channel, are of class-weight one, then construction of codes correcting these error-patterns by the method given in this section, gives code words having length twice the length of the code words in single-error-correcting Hamming codes, where all other parameters (different from length) are same in the two codes.

Example. Let $q = 19$, $B_1 = \{1,2,3,16,17,18\}$,

r = number of parity checks = 2. Then the parity check matrix constructed by the method given in this section, of the code, which is capable of correcting any error with value as 1, 2, 3, 16, 17 or 18 in a single position, is given by

$$\begin{array}{lccccccccccc}
\text{Position number} & 1 & 2 & 3 & 4 & \dots & 21 & 22 & 23 & \dots & 39 & 40 \\
\multirow{2}{*}{H =} & 0 & 0 & 1 & 1 & \dots & 1 & 4 & 4 & \dots & 4 & 4 \\
 & 1 & 4 & 0 & 1 & \dots & 18 & 0 & 1 & \dots & 17 & 18
\end{array}$$

The code which has H as its parity-check matrix, is of length 40, whereas the corresponding single-error-correcting Hamming code has length 20.

3.2.1 Another Class of Parity Check Matrices for Single-Class-Error-Correcting Codes

We give another method of constructing a parity check matrix for a code of length n, which uses r parity checks and is capable of correcting all error patterns of class-weight one. The method of construction of these codes is on the lines of those followed by Berlekamp ((1968), page 208) in constructing codes correcting errors of ±1 in a single place (i.e., errors of Lee-weight one). This method uses the idea of labeling different digits of the code with nonzero element) in an extension field of Z_q, the code alphabet, where q is a prime number. As mentioned earlier, class-metric under consideration is determined by a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots., B_{m-1}\}$ of Z_q.

Construction: Let K be the smallest multiplicative subgroup (having least possible number of elements) of $Z_q \sim \{0\}$, which contains B_1. Then the length of the code (to be constructed) using r parity check symbols is given by

$$n = \frac{(q^r - 1)}{|k|}, \qquad \ldots \text{(eq 3.11)}^1$$

Where $|K|$ is the number of elements in K.

Let α be a primitive element of an extension field F of degree r, of Z_q and

[1] R H S in eq 3.11 is a natural number as $|K|$, the number of elements in a sub group divides the number of elements in the group (i.e. q^{r-1}).

$$H = [1, \alpha, \ldots, \alpha^{n-1}] \qquad \text{... (eq 3.12)}$$

be the parity check matrix of a code C_H, where n is given by (eq 3.11).

For the code C_H to be capable of correcting all error patterns of class-weight one, all such error patterns should have distinct syndromes. This will be true, if we are able to show that

$$a\alpha^i \neq b\alpha^j,$$

for $a, b \in B_1$, $a \neq b$ and $1 \leq i, j \leq n-1$.

Let us consider

$$a\alpha^i = b\alpha^j, \quad \text{for } i, j = 1, 2, \ldots.., n-1 \text{ and } a \neq b$$

i.e. $\alpha^{i-j} = a^{-1}b$ ... (eq 3.13)

Assuming that i is greater than or equal to j, we get

$$0 \leq i\text{-}j \leq n\text{-}1.$$

Then

$$(i-j)|k| < n.|k| = \frac{q^r - 1}{|k|}|\,k\,| = q^r - 1 \quad \text{(from (eq 3.11))}$$

Therefore

$(i-j)\ |K| < q^r-1.$ ... (eq 3.14)

Now a and b being elements of B_1, are elements of K. Therefore $a^{-1}b$ is an element of K and hence α^{i-j} is an element of K. This is true if and only if

$\alpha^{i-j} = \alpha^0 = 1$ (because of (eq 3.14 and α^t=K or disticnct for $0 \leq t < n$)

Therefore, from (eq 3.13), we get

$$a = b,$$

which is in contradiction to what we assumed. Thus

$$a\alpha^{-1} \neq b\alpha^j .$$

Decoding: As in the previous case, we calculate the syndrome $\underline{c}\ H^T$ of the received vector $\underline{c}$.

If $\underline{c}H^T$ is the null vector then we assume that $\underline{c}$ is the transmitted code word. Otherwise $\underline{c}H^T$ is equal to $a.\alpha^i$, the syndrome of some error pattern having an entry a of class-weight one in $(i+1)^{th}$ position. As syndrome of error patterns of class-weight one are distinct, therefore, an error pattern of class-weight one is determined uniquely. Subtracting the error pattern from the received vector, we get the transmitted vector (assuming class-weight of error patterns does not exceed one).

Next we give an example to explain these ideas.

Example : Let $q = 31$, r = number of parity checks = 2, and
$B_1 = \{1, 2, 29, 30\}$.

Then K, the smallest subgroup of $Z_{31} \sim \{0\}$ containing B_1, is such that

$K = [29]$ = subgroup generated by the element 29 of $Z_{31} \sim \{0\}$

and $|K|$ = order of 29 in the multiplicative group $Z_{31} \sim \{0\} = 10$.

Then n, the length of the desired code is given by

$$N = (31^2-1)/10 = 96$$

Let α be a primitive element of the field F, an extension of degree 2 over Z_{31}. Then the parity-check matrix of a code correcting all error patterns having entries 1, 2, 29 or 30 in a single place is given by

$$H = [1, \alpha, \ldots, \alpha^{n-1}].$$

Remarks: The last class of codes constructed above, corrects not only error patterns having class-weight one, but all error patterns having an entry from K in a single place, K being the smallest multiplicative subgroup of $Z_q \sim \{0\}$ containing B_1. These codes are more useful in the case when number of elements in K is comparatively much smaller than number of elements in Z_q. Otherwise, Hamming codes correcting single error, are more suitable. It may be noted that if

$$B_1 = \{\pm 1\} \text{ then } K = B_1,$$

and the class of codes constructed above coincides with the class of Lee-metric codes correcting ±1 in a single place, given in Berlekamp (1968). Again if

$$B_1 = \{1,2,\ldots,q-1\},$$

then B_1 coincides with K and codes constructed above are *single-Hamming-error-correcting codes.* In only these two situations, B_1 coincides with K.

We mentioned in Chapter I that the subject of error-correcting codes had arisen because of practical needs. Therefore, it is important to evaluate the performance of a code, which in the case of random errors is judged in terms of minimum distance and/or number of parity checks used, when the channel is not specified (i.e., is arbitrary). As it is not possible always to find minimum distance or number of parity checks used, therefore bounds are derived on these. Hamming bound (c.f. Hamming, 1950), Plotkin bound (c.f. Plotkin, I960) and Varshamov-Gilbert-Sacks bound (c.f., Peterson and Weldon, 1972) are some well-known bounds for Hamming metric codes. In the next sections, we will find similar bounds for codes correcting random errors on class-metric channels. In Section 3.3, we discuss only upper bounds.

3.3 Hamming-Type and Plotkin-Type Bounds

Let $\mathcal{P}_1 = \{B_0, B_1, ..., B_{m-1}\}$ be a $\mathcal{P}$-partition of Zq, which determines the class-metric, which we use in our considerations. Upper bounds on minimum class-distances are obtained by employing the technique of sphere-packing due to Hamming (1950) and that of taking average due to Plotkin (1960). For this, we require extensions of the notions of a sphere, surface area of a sphere and volume of a sphere, (c.f. Berlekamp, 1968), given already for Hamming and Lee metrics, to chose for class-metrics. For these definitions and in Theorem 3.2, q may be any positive integer not necessarily a prime.

Definition: The set of all n-tuples over Zq, having class-distances from a fixed n-tuple, less than or equal to a non-negative integer t is called a *sphere of class-radius t.* The fixed point is called the centre of the sphere.

Definition: The surface area of a *sphere of class-radius t* denoted by $A^{(n)}_{t,\mathcal{P}_1}$, is the number of n-tuples having class-distance t from the center.

Definition: The volume of the sphere of class-radius t, denoted by $V^{(n)}_{t,\mathcal{P}_1}$, is the number of n-tuples having class-distance less than or equal to t.

Clearly:

$$V^{(n)}_{t,\mathcal{P}_1} = \sum_{i=0}^{t} A^{(n)}_{i,\mathcal{P}_1} \qquad \text{... (eq 3.15)}$$

$A^{(n)}_{i,\mathcal{P}_1}$ denote all n-tuples which have exact i class-weight, where as

$V^{(n)}_{t,\mathcal{P}_1}$ denote n-tuple which have class weight t or less.

Generating Functions: To find out the values of $A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t,\mathcal{P}_1}$ for given values of n and t and for a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, we consider the following generating function

$$A^{(n)}_{\mathcal{P}_1}(z) = \sum_{i=0}^{\infty} A^{(n)}_{i,\mathcal{P}_1} z^i . \qquad \text{... (eq 3. 16)}$$

Since the class-distance is additive over n (refer eq 2.2), the generating function $A^{(n)}_{\mathcal{P}_1}(z)$ is multiplicative over n positions and hence

$$A^{(n)}_{\mathcal{P}_1}(z) = \left[A^{(1)}_{\mathcal{P}_1}(z)\right]^n = \left[1 + n_1 z + \ldots + n_{m-1} z^{m-1}\right]^n, \qquad \text{... (eq 3.17)}$$

Where

$$|B_i| = n_i \text{ and m is the number of classes in } \mathcal{P}_1$$

The multinomial expansion, (refer Riordon, 1958), of R.H.S. of (eq 3.17), on comparison with (eq 3.16), gives

$$A^{(n)}_{t;\mathcal{P}_1} = \sum_{s_i} \frac{n!}{s_0! s_1! \ldots s_{m-1}!} n_1^{s_1} \ldots n_{m-1}^{s_{m-1}},$$

Where

$$s_0 + s_1 + \ldots + s_{m-1} = n \text{ (number of positions in n-tuple)}$$

and

$$0.s_0 + 1.s_1 + 2.s_2 + \ldots + (m-1)s_{m-1} = t$$

Now

$V^{(n)}_{T,\mathcal{P}_1}$ can be calculated by summing $A^{(n)}_{t,\mathcal{P}_1}$ over t, $0 \le t \le T$, (refer eq 3.15).

For convenience of reference in future, we state the results giving the values of $A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t,\mathcal{P}_1}$ in the form of the following theorem.

Theorem 3.2: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$of Z_q determining the class-metric under consideration, and two non-negative integers n and t, $n \ge 1$; $A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t,\mathcal{P}_1}$ the set of all n-tuples having class-distances respectively equal to t and less than or equal to t, from a fixed n-tuple, are given by

$$A^{(n)}_{t,\mathcal{P}_1} = \sum_{s_i} \frac{n!}{s_0!\, s_1! \ldots s_{m-1}!}\, n_1^{s_1} \ldots n_{m-1}^{s_{m-1}}$$

where

$$|B_i| = n_i \qquad \ldots \text{(eq 3.18)}$$

and s_i's satisfy

$$s_0 + s_1 + \ldots . s_{m-1} = n \text{ and } s_1 + 2s_2 + \ldots . + (m-1)s_{m-1} = t$$

and

$$V^{(n)}_{t,\mathcal{P}_1} = \sum_{s_i} \frac{n!}{s_0!\,s_1!\ldots s_{m-1}!}\; n_1^{s_1} n_2^{s_2} \ldots n_{m-1}^{s_{m-1}}$$

Where

s_i's satisfy

$s_0 + s_1 + \ldots + s_{m-1} = n$ and ... (eq 3.19)

$s_1 + 2s_2 + \ldots + (m-1)s_{m-1} \leq t$

respectively.

Explanation: In case either $n \leq 0$ and/or $t < 0$, the spheres with these parameters are non-existing. We will assume that

$$A^{(n)}_{t,\mathcal{P}_1} = 0 \quad \text{and} \quad V^{(n)}_{t,\mathcal{P}_1} = 0$$

If $\quad n \leq 0 \quad$ and/or $\quad t < 0$ ... (eq 3.20)

Further, class-distance of an n-tuple cannot exceed n(m-1) from another n-tuple (say the center of the sphere), therefore

$$A^{(n)}_{t,\mathcal{P}_1} = 0 \text{ and } V^{(n)}_{t,\mathcal{P}_1} = V^{(n)}_{n(m-1),\mathcal{P}_1} = q^n$$

for $t > n(m-1)$ ... (eq 3. 21)

Corollary 3.1: In the case of Hamming metric, we have m-1 = 1 and

$$\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\},$$

where $B_1 = \{1,2,\ldots\ldots\ldots\ldots, q-1\}$,

and thus $\left|B_1\right| = q - 1$

Therefore

$$A^{(n)}_{t,\mathcal{P}_H} = \binom{n}{t}(q-1)^t \qquad \text{... (eq 3.22)}$$

and

$$V^{(n)}_{t,\mathcal{P}_H} = \sum_{s=0}^{t}\binom{n}{s}(q-1)^s \qquad \text{... (eq 3.23)}$$

Corollary 3.2: In the case of Lee metric, q an odd positive integer, we have

$$m-1 = (q-1)/2, \qquad \mathcal{P}_1 = \mathcal{P}_L = \{B_0, B_1, \ldots\ldots\ldots, B_{(q-1)/2}\},$$

where $B_i = \{i, q-i\}$ for $i = 1,2\ldots\ldots\ldots\ldots\ldots,\frac{(q-1)}{2}$

Therefore

$$\left|B_i\right| = 2 \text{ for all } i\,.$$

Thus

$$\left.\begin{aligned}
A^{(n)}_{t,\mathcal{P}_L} &= \sum_{s_i} \frac{n!}{s_0!\,s_1!\ldots s_{(q-1)/2}!}2^{n-s_0} \\
&= 2^n n! \sum_{s_i} \frac{1}{s_0!\,s_1!\ldots s_{(q-1)/2}!}\,\frac{1}{2^{s_0}}, \\
&\text{Where} \\
&s_0 + s_1 + \ldots + s_{(q-1)/2} = n \quad \text{and} \\
&s_1 + 2s_2 + \ldots + \frac{(q-1)}{2} s_{\frac{(q-1)}{2}} = t
\end{aligned}\right\} \qquad \ldots \text{(eq 3.24)}$$

and

$$\left.\begin{aligned}
&V^{(n)}_{t,\mathcal{P}_L} = 2^n n! \sum_{s_i} \frac{1}{s_0!s_1!\ldots s_{(q-1)/2}!}\,\frac{1}{2^{s_0}} \\
&\text{where} \\
&s_0 + s_1 + \ldots + s_{(q-1)/2} = n \text{ and} \\
&s_1 + 2s_2 + \ldots + \left(\frac{q-1}{2}\right) s_{(q-1)/2} \le t
\end{aligned}\right\} \qquad \ldots \text{(eq 3.25)}$$

For even q, the values of $A^{(n)}_{t,\mathcal{P}_L}$ and $V^{(n)}_{t,\mathcal{P}_L}$ may be obtained with minor modifications. However in this thesis we require these values only for q an odd integer.

For the sake of convenience of notations and reference we introduce the notion of a spherical hull.

Definition: The set of all n-tuples having class-distances from a fixed n-tuple (the center) less than or equal to t_1 and greater than t_2 (with $t_1 \geq t_2$), is called a spherical hull of radii t_1 and t_2.

Definition: The volume of a spherical hull, denoted by $V^{(n)}_{t_1,t_2,\mathcal{P}_1}$, is the set of all n-tuples having class-distances less than or equal to t_1 and greater than t_2 from the center.

Clearly

$$\left.\begin{aligned} &V^{(n)}_{t_1,t_2,\mathcal{P}_1} = V^{(n)}_{t_1,\mathcal{P}_1} - V^{(n)}_{t_2,\mathcal{P}_1} \quad \text{for } t_1 \geq t_2 \\ &\text{and} \\ &V^{(n)}_{t_1,t_2,\mathcal{P}_1} = 0 \qquad \text{for } t_1 < t_2 \end{aligned}\right\} \quad \ldots \text{(eq 3.26)}$$

3.3.1 Hamming-Type Bound

The following bound is true in the case of even non-linear codes.

Theorem 3.3: Given a $\mathcal{P}$-partition $\mathcal{P}_1$ = {B_0, B_1......, B_{m-1}} of Z_q determining the class-metric under consideration, the number of code words M in a code capable of correcting every error pattern of class-weight t or less, satisfies

$$M \leq \frac{q^n}{V^{(n)}_{t,\mathcal{P}_1}} \qquad \text{... (eq 3.27)}$$

Proof: For a code to be capable of correcting error patterns of class-weight t or less, the spheres of class-radii t or less having the codewords as their centers should be disjoint. Therefore

$$MV^{(n)}_{t,\mathcal{P}_1} \leq q^n, \qquad \text{... (eq 3.28)}$$

from which follows (eq 3.27).

3.3.2 Plotkin-Type Bound

In the next theorem, a bound on number of parity checks is obtained by calculating the average weight of code words (c.f. Plotkin, 1960). For the main result we require the following two lemmas:

Lemma 3.1: Given a $\mathcal{P}$-partition $\mathcal{P}_1$ = {B_0, B_1, ..., B_{m-1}} of Z_q, q prime, determining the class-weight under consideration, the minimum class-distance $d_{\mathcal{P}_1}$ of an (n, k) linear code over Z_q, does not exceed

$$\frac{nq^{k-1}W(\mathcal{P}_1)}{q^k - 1}, \qquad \text{... (eq 3.29)}$$

Where $\quad W(\mathcal{P}_1) = \sum_{i=1}^{m-1} i|B_i|,$

is the sum of the class-weights of the letters of the alphabet {0,1,....q-1}.

Proof: Arrange all the code words as rows of a matrix in such a way that no column contains all zeros. Then, (c.f. Peterson and Weldon (1972), Problem 3.5), each field element appears q^{k-1} times in each column. Therefore, the sum of class-weights of the code words of the given (n, k) linear code is

$$nq^{k-1}\{1|B_1| + 2|B_2| + ...(m-1)|B_{m-1}|\}$$

$$= nq^{k-1}W(\mathcal{P}_1).$$

The proof follows from the fact that the minimum never exceeds the average.

Let $B_{\mathcal{P}_1}(n,d)$ denote the size of the maximal linear code of length n and minimum class-distance d. Then

Lemma 3.2: If n > d,

$$B_{\mathcal{P}_1}(n,d) \leq qB_{\mathcal{P}_1}(n-1,d).$$

Proof: Let C_1 be a linear code having length n, minimum class-distance d and number of code words equal to $B_{\mathcal{P}_1}(n,d)$. Then the set of all the code words of C_1 which have zero as their last component form a subspace C_2 of C_1 having $\frac{1}{q}B_{\mathcal{P}_1}(n,d)$ number of code words from C_1. If we drop last components from each member of C_2 we get a code of length (n-1) with minimum class-distance d and number of code words equal to $\frac{1}{q} B_{\mathcal{P}_1}(n, d)$. Hence

$$B_{\mathcal{P}_1}(n - 1, d) \geq \frac{1}{q} B_{\mathcal{P}_1}(n, d)$$

proving thereby the lemma.

Theorem 3.4: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration, and $n \geq (qd - 1) / W(\mathcal{P}_1)$, the number of parity-check symbols required to achieve minimum class-distance d in an n-symbol linear code over Z_q, q prime, is at least

$$\frac{qd - 1}{W(\mathcal{P}_1)} - 1 - \log_q d \qquad \ldots \text{(eq 3.30)}$$

where

$$W(\mathcal{P}_1) = \sum_{i=1}^{m-1} i|B_i|$$

Proof: Applying lemma 3.1 to a linear code of length i having k information symbols, we get

$$d \leq \frac{i\, q^{k-1} W(\mathcal{P}_1)}{q^k - 1},$$

i.e. $(q^k - 1)d \leq iq^{k-1} W(\mathcal{P}_1)$

i.e. $q^{k-1}\left(qd - iW\left(\mathcal{P}_1\right)\right) \le d$

and if

$$qd - i\,W(\mathcal{P}_1) > 0$$

then

$$q^{k} \le \frac{qd}{qd - iW(\mathcal{P}_1)} \qquad \text{... (eq 3.31)}$$

Let $i = \left\lfloor \left(qd - 1\right) / W\left(\mathcal{P}_1\right) \right\rfloor$

$$\frac{(qd-1)}{W(\mathcal{P}_1)} = i + f \qquad \text{for } 0 \le f < 1 \qquad \text{... (eq 3.32)}$$

then

$$qd = W(\mathcal{P}_1)(i+f) + 1.$$

Substituting this value of qd in the denominator of R.H.S. in (eq 3.31) we get

$$B_{\mathcal{P}_1}(i, d)\left(= q^{k}\right) \le \frac{qd}{\left(1 + W\left(\mathcal{P}_1\right)f\right)}$$

In case $n \ge i$, applying Lemma 3.2 we get

$$B_{\mathcal{P}_1}(n, d) \le q^{n-i} B_{\mathcal{P}_1}(i, d)$$

$$\le q^{n-\{(qd-1)/W(\mathcal{P}_1)\}+f} \frac{qd}{(1 + W(\mathcal{P}_1)f)} \qquad \text{... (eq 3.33)}$$

(substituting the value of i from (eq 3.32)).

Also $q^f \le 1 + (q-1)f \le q + W(\mathcal{P}_1)f \quad (W(\mathcal{P}_1) \ge q\text{-}1)$

Using this inequality in (eq 3.33), we get

$$B_{\mathcal{P}_1}(n, d) \le q^{n-\{(qd-1)/W(\mathcal{P}_1)\}+f} qd / q^f$$

i.e.

$$B_{\mathcal{P}_1}(n, d) \le q^{n-\{(qd-1)/W(\mathcal{P}_1)\}} qd.$$

Since $B_{\mathcal{P}_1}(n, d) = q^k$ for the code with maximum minimum distance, where k is the number of information symbols for that code, we have

$$k \le n - \frac{qd - 1}{W(\mathcal{P}_1)} + 1 + \log_q d,$$

from which (eq 3.30) follows directly.

Remarks: The corresponding results for Hamming and Lee metrics can be directly obtained from Theorem 3.4 as follows:

For Hamming metric, we have

$$W(\mathcal{P}_H) = q - 1 \qquad \text{... (eq 3.34)}$$

Using (eq 3.34), Theorem 3.4 reduces to Theorem 4.1 of Peterson and Weldon (1972).

Next, for Lee metric

$$W(\mathcal{P}_L) = \frac{(q^2 - 1)}{4} \quad \text{for q an odd prime} \qquad \text{... (eq 3.35)}$$

Using (eq 3.35), the result of Theorem 3.4 reduces to the following

Corollary 3.3: If $n \geq 4(qd - 1)/(q^2 - 1)$, q an odd prime, the number of parity-check symbols required to achieve minimum Lee-distance d in an (n, k) linear code is at least

$$\left\{\frac{4(qd - 1)}{(q^2 - 1)}\right\} - 1 - \log_q d$$

3.4 Varshamov-Gilbert-Like Bound

In this section, we derive Varshamov-Gilbert-type bound on sufficient number of parity checks required in codes correcting a given number of random errors on class-metric channels. The method adopted is on the line of that given by Sacks (1958) for deriving Varshamov-Gilbert bound. This is taken up in the next theorem.

Theorem 3.5: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots\ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration, it is always possible to construct an (n, k) linear code with minimum class-distance d, if the following inequality holds

$$V^{(n)}_{d-2,\mathcal{P}_1} \geq q^{n-k} \qquad \text{... (eq 3.36)}$$

where $V^{(n)}_{d-2,\mathcal{P}_1}$ is given by (eq 3.19).

Proof: The existence of such a code will be shown by constructing an appropriate (n-k)×n parity-check matrix H.

A nonzero (n-k)-tuple may be chosen as the first column of H (c.f. Theorem 4.7, Peterson and Weldon, 1972). Subsequent columns may be added such that after having selected j-1 columns $h_1, h_2, \ldots\ldots, h_{j-1}$, a column h_j is added provided that it is not a *linear combination of class-weight d-2 or less of the columns* from amongst the previous columns. In the worst possible case, when all the linear combinations of class-weight d-2 or less of the columns from amongst the previous j-1 columns, are distinct; their number being equal to the number of all nonzero (j-1)-tuples of class-weight d-2 or less, is

$$V^{(j-1)}_{d-2,\mathcal{P}_1} - 1 \text{ (excluding the all-zero vectors)}$$

For j ≤ n, the set of all the $q^{n-k}-1$ nonzero (n-k)-tuples will not be exhausted provided that

$$V^{(j-1)}_{d-2,\mathcal{P}_1} - 1 < q^{n-k} - 1 \qquad \text{... (eq 3.37)}$$

If n is the largest value of j for which inequality (eq 3.37) holds, an (n, k) linear code will exist satisfying (eq 3.36).

In the case of Hamming metric, using (eq 3.23), it easily follows that Theorem 3.5 given above reduces to Theorem 4.7 of Peterson and Weldon (1972).

In the case of Lee metric Theorem 3.5 can be stated as

Corollary 3.4: It is always possible to construct an (n, k) linear code over Z_q, q an odd prime, with minimum Lee distance d if the following inequality holds

$$V^{(n)}_{d-2,\mathcal{P}_l} \geq q^{n-k}, \qquad \text{... (eq 3.38)}$$

where $V^{n}_{d-2,\mathcal{P}_l}$ is given by (eq 3.25).

3.5 Codes detecting/Correcting Random Errors Having Constraint on Magnitude of Error in a Position and/or Number of Error Positions

The formulation of a problem of detection or correction of errors arising out of a faulty communication channel is essentially based on the notion of error-metric. Golomb (1962) gave a systematic treatment of the general class of metrics that might reasonably correspond to the error patterns which are encountered in actual communication system.

The treatment is based on the idea of a general error sphere in the space of n-tuples. More precisely, for an n-tuple A = $(a_1,.........,a_n)$ over an alphabet set Z_q and a weight function in Z_q^n, a sphere $S_{hml}(A)$ is defined as the set of all the n-tuples B = $(b_1,......,b_n)$ over Z_q for which

i) a_i is different from b_i for at most h i's, i.e., number of places in which A and B differ is at most h;

ii) the weight of the difference in each of the corresponding entries in A and B does not exceed m, i.e. $\|a_i - b_i\| \leq m$ for i=1,...,n ; and

iii) The sum of the weights of the differences in all the co-ordinates does not exceed *l*.

The significance of the idea is that it helps in reducing the number of parity-check symbols and hence in increasing the efficiency of the communication systems, in situations where either the number of positions in which errors occur is small as compared to the code length and/or the magnitude of errors in each of the different positions is less than the maximum magnitude possible in a position. These situations may be seen arising in practical when we dial a number on the telephone. In normal circumstances, the number of digits, which are received incorrectly, is small as compared to that are in the number dialed. Even in the case of receiving wrong digit, it may not deviate much from the digit sent, e.g., if we dial 5 on the telephone, then in the case of faulty instrument which suppresses or picks up at the most two pulses, what can be received is only 3,4,5,6, or 7 and no other digit.

For such situations, it will be wastage of resources to devise codes correcting errors having no restriction on number of error positions and/or on the magnitude of error in a position. Because then the code will have inbuilt property of correcting even those errors which are not going to arise at all. This will amount to having more parity-check digits than in fact suffice by making use of the above idea due to Golomb (1969).

In the case of Hamming metric, the notion of restricted magnitude of an error position is irrelevant as every nonzero position has weight one. But for a class-metric other than Hamming, we can think of imposing this condition on error vectors.

Sharma and Goel (1978) have made investigations about codes having restrictions on number of error positions and/or magnitude of an error position with reference to Lee metric. They have introduced the notion of *Limited Intensity* of noise for Lee metric, that is based on magnitude or on an error position.

In this section we propose to obtain lower and upper bounds on respectively the necessary and sufficient number of parity-check symbols required in codes correcting random errors with restrictions on number of positions and/or magnitude of an error position. These bounds are derived with reference to a class-metric.

The studies require introduction of some definitions. First we extend the idea of "Limited Intensity" to class-metric codes.

Definition: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1 \ldots\ldots, B_{m-1}\}$ of Z_q determining a class metric under consideration in the space of n-tuples over Z_q, and that the vector $\underline{v} = (b_1, b_2, \ldots, b_n), b_i \in Z_q$ is received when the vector $\underline{u} = (a_1, a_2, \ldots, a_n), a_i \in Z_q$ is transmitted. Then *intensity of noise* is given by

$$\max_{1 \le i \le n} \left[d_{\mathcal{P}_1}(a_i, b_i) \right].$$

Further, a vector $\underline{u} = (a_1, a_2, \ldots, a_n)$ will be said to have *intensity* a if

$$\max_{1 \le i \le n} \left[w_{\mathcal{P}_1}(a_i) \right] \le a .$$

Next we define some specific purpose error-spheres on the lines suggested by Golomb (1969).

Definition: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1 \ldots\ldots, B_{m-1}\}$ of Z_q, determining the class-metric under consideration in the space of n-tuples over Z_q, we define a *b-position sphere of class-radius t* with center $\underline{u} = (a_1, a_2, \ldots, a_n)$ as the set of all n-tuples $\underline{v} = (b_1, b_2, \ldots, b_n)$ over Z_q for which the following two conditions hold:

i) $a_i \neq b_i$ for most b i's

and ii) $d_{\mathcal{P}_1}(\underline{u}, \underline{v}) \le t$

Thus sphere is denoted by $S^{(n,b)}_{t,\mathcal{P}_1}(\underline{u})$.

Further, a ‘*sphere of class-radius t and intensity limited by a*’ with center $\underline{u} = (a_1, a_2, \ldots, a_n)$ is defined as the set of all n-tuples $\underline{v} = (b_1, b_2, \ldots, b_n)$ for which in addition to condition ii) given above, the following condition

iii) $\quad d_{\mathcal{P}_1}(a_i, b_i) \leq a \qquad$ for $i = 1,2,\ldots,n$

is satisfied. (However, condition (i) may not be satisfied)

We denote this sphere by $S^{(n),a}_{t,\mathcal{P}_1}(\underline{u})$.

Next we define a ‘*b-position sphere of class-radius t and intensity limited by a*’ with center $\underline{u} = (a_1, a_2, \ldots, a_n)$ as the set of all n-tuples $\underline{v} = (b_1, b_2, \ldots, b_n)$which satisfy conditions (i), (ii) and (iii) given above.

This sphere is denoted by $S^{(n,b),a}_{t,\mathcal{P}_1}(\underline{u})$.

In our studies we do not require the center $\underline{u}$ and hence we may drop $\underline{u}$ from the notations, and hence the spheres

defined above will be denoted respectively by $S^{(n,b)}_{t,\mathcal{P}_1}$, $S^{(n),a}_{t,\mathcal{P}_1}$ and $S^{(n,b),a}_{t,\mathcal{P}_1}$.

The surface areas of the spheres $S^{(n,b)}_{t,\mathcal{P}_1}$, $S^{(n),a}_{t,\mathcal{P}_1}$ and $S^{(n,b),a}_{t,\mathcal{P}_1}$ denoted respectively by $A^{(n,b)}_{t,\mathcal{P}_1}$, $A^{(n),a}_{t,\mathcal{P}_1}$ and $A^{(n,b),a}_{t,\mathcal{P}_1}$ are the numbers of n-tuples in the respective spheres whose class-distances from the centers are exactly t.

Also the volume of the spheres $S^{(n,b)}_{t,\mathcal{P}_1}$, $S^{(n),a}_{t,\mathcal{P}_1}$ and $S^{(n,b),a}_{t,\mathcal{P}_1}$ denoted respectively by $V^{(n,b)}_{t,\mathcal{P}_1}$, $V^{(n),a}_{t,\mathcal{P}_1}$ and $V^{(n,b),a}_{t,\mathcal{P}_1}$ are the numbers of n-tuples in the respective spheres.

It is a straightforward matter to see that A's and V's defined above are independent of the center of the sphere. Hence we may calculate A's and V's by taking origin as the centre.

Then proceeding on the lines of method adopted in determining $A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t,\mathcal{P}_1}$ given in Theorem 3.2, we can determine the values for different A's and V's considered above. These values are given in the form of the next theorem for the convenience of the future references.

Theorem 3.6: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q and non-negative integers n, t, b and a, such that $1 \leq a \leq m-1$; $b \leq n$, $t \leq (m-1)n$, then $A^{(n,b)}_{t,\mathcal{P}_1}$, the number of n-tuples over Z_q having at most b nonzero entries and that are of class-weight t is given by

$$\left.\begin{aligned} & A^{(n,b)}_{t,\mathcal{P}_1} = \sum_{s_i} \binom{n}{b} \frac{b!}{s_0!s_1!,\ldots,s_{m-1}!} n_1^{s_1} \ldots n_{m-1}^{s_{m-1}} \\ & \text{where } |B_i| = n_i \text{ and } s_i\text{'s satisfy} \\ & \qquad s_0 + s_1 + \ldots + s_{m-1} = b \\ & \text{and} \quad s_1 + 2s_2 + \ldots + (m-1)s_{m-1} = t. \end{aligned}\right\} \quad \ldots \text{(eq 3.39)}$$

Then $V^{(n,b)}_{t,\mathcal{P}_1}$, the number of n-tuples over Z_q having at most b nonzero entries and class-weight t or less is given by

$$V^{(n,b)}_{t,\mathcal{P}_1} = \sum_{i=0}^{t} A^{(n,b)}_{i,\mathcal{P}_1} \qquad \ldots \text{(eq 3.40)}$$

Also

$A^{(n),a}_{t,\mathcal{P}_1}$ the number of n-tuples over Z_q having class-weight t and intensity limited by a (i.e. none of the n-tuples has an entry of class-weight more than a), is given by

$$\left.\begin{aligned}
&A^{(n),a}_{t,\mathcal{P}_1} = \sum_{s_i} \frac{n!}{s_0!s_1!,\ldots,s_a!} n_1^{s_1} \ldots . n_a^{s_a} \\
&\text{where } \left|B_i\right| = n_i \text{ and} \\
&s_0 + s_1 + \ldots + s_a = n \\
&\text{and } s_1 + 2s_2 + \ldots + as_a = t.
\end{aligned}\right\} \ldots \text{(eq 3.41)}$$

Then $V_{t,\mathcal{P}_1}^{(n),a}$, the number of n-tuples over Z_q having class-weight t or less and intensity limited by a is given by

$$V_{t,\mathcal{P}_1}^{(n),a} = \sum_{i=0}^{t} A_{i,\mathcal{P}_1}^{(n),a} \qquad \text{... (eq 3.42)}$$

Further

$A_{t,\mathcal{P}_1}^{(n,b),a}$, the number of n-tuples over Z_q with intensity limited by a having class-weight t and in which number of nonzero entries does not exceed b, is given by

$$\left.\begin{array}{l} A_{t,\mathcal{P}_1}^{(n,b),a} = \sum\limits_{s_i} \binom{n}{b} \dfrac{b!}{s_0!s_1!,\ldots,s_a!} n_1^{s_1} \ldots n_a^{s_a} \\[2ex] \text{where} \quad |B_i| = n_i \text{ and } s_i\text{'s satisfy} \\[2ex] s_0 + s_1 + \ldots + s_a = b \\[2ex] \text{and} \quad s_1 + 2s_2 + \ldots + as_a = t. \end{array}\right\} \qquad \text{... (eq 3.43)}$$

$V_{t,\mathcal{P}_1}^{(n,b),a}$, the number of n-tuples over Z_q with intensity limited by 'a' having class-weight t or less and in which number of nonzero entries does not exceed b is given by

$$V^{(n,b),a}_{t,\mathcal{P}_1} = \sum_{i=0}^{t} A^{(n,b),a}_{i,\mathcal{P}_1} \qquad \text{... (eq 3.44)}$$

Remarks: For $n \leq 0$ and/or $t < 0$ all the numbers A's and V's considered above are assumed to be zero. Also for $n \geq 1$

i) If $t > b(m-1)$ then

$$A^{(n,b)}_{t,\mathcal{P}_1} = 0 \qquad \text{... (eq 3.45)}$$

and $$V^{(n,b)}_{t,\mathcal{P}_1} = V^{(n,b)}_{b(m-1),\mathcal{P}_1} \qquad \text{... (eq 3.46)}$$

ii) if $t > na$, then

$$A^{(n),a}_{t,\mathcal{P}_1} = 0 \quad \text{and} \quad V^{(n),a}_{t,\mathcal{P}_1} = V^{(n),a}_{na,\mathcal{P}_1} \qquad \text{... (eq 3.47)}$$

iii) if $t > ba$, then

$$A^{(n,b),a}_{t,\mathcal{P}_1} = 0 \text{ and } V^{(n,b),a}_{t,\mathcal{P}_1} = V^{(n,b),a}_{ba,\mathcal{P}_1} \qquad \text{... (eq 3.48)}$$

iv) if $b = n$ then

$$A^{(n,n)}_{t,\mathcal{P}_1} = A^{(n)}_{t,\mathcal{P}_1} \quad \text{and} \quad V^{(n,n)}_{t,\mathcal{P}_1} = V^{(n)}_{t,\mathcal{P}_1}$$

and v) if $a = m - 1$ then

$$A^{(n),m-1}_{t,\mathcal{P}_1} = A^{(n)}_{t,\mathcal{P}_1} \quad \text{and} \quad V^{(n),m-1}_{t,\mathcal{P}_1} = V^{(n)}_{t,\mathcal{P}_1}$$

In the case of Hamming metric, a = 1 and b = t and hence

$$A^{(n,t)}_{t,\mathcal{P}_H} = A^{(n),1}_{t,\mathcal{P}_H} = A^{(n,t),1}_{t,\mathcal{P}_H} = A^{(n)}_{t,\mathcal{P}_H} \quad \text{and}$$

$$V^{(n,t)}_{t,\mathcal{P}_H} = V^{(n),1}_{t,\mathcal{P}_H} = V^{(n,t),1}_{t,\mathcal{P}_H} = V^{(n)}_{t,\mathcal{P}_H} .$$

In the case of Lee metric when q is odd, m-1 = (q-1)/2 and $|B_i| = n_i = 2$.

Then the numbers A's and V's considered in Theorem 3.6 become

$$\left.\begin{array}{l} A^{(n,b)}_{t,\mathcal{P}_L} = \sum\limits_{s_i} \binom{n}{b} \dfrac{b!}{s_0!s_1!..s_{(q-1)/2}!} \dfrac{2^b}{2^{s_0}}, \\[2em] \text{where } s_0 + s_1 + \ldots + s_{(q-1)/2} = b \\[2em] \text{and } s_1 + 2s_2 + \ldots + \dfrac{(q-1)}{2} s_{(q-1)/2} = t \end{array}\right\} \quad \ldots \text{(eq 3.49)}$$

$$\left.\begin{array}{l} A^{(n),a}_{t,\mathcal{P}_L} = \sum\limits_{s_i} \dfrac{n!}{s_0!s_1!..s_a!} \dfrac{2^n}{2^{s_0}}, \\[2em] \text{where } s_0 + s_1 + \ldots + s_a = n \\[2em] \text{and } s_1 + 2s_2 + \ldots + as_a = t \end{array}\right\} \quad \ldots \text{(eq 3.50)}$$

and

$$\left.\begin{aligned} A^{(n,b),a}_{t,\mathcal{P}_L} &= \sum_{s_i}\binom{n}{b}\frac{b!}{s_0!s_1!..s_a!}\,\frac{2^b}{2^{s_0}}, \\ \text{where}\quad & s_0+s_1+\ldots+s_a = b \\ \text{and}\quad & s_1+2s_2+\ldots+as_a = t \end{aligned}\right\} \qquad \ldots(\text{eq } 3.51)$$

and the $V_{t,\mathcal{P}_L}$'s can be obtained by taking summation over the corresponding $A_{i,\mathcal{P}_L}$'s for i varying from 1 to t.

For even q we may find values of A's and V's with minor modifications in the above arguments.

The Hamming-type bounds and Varshamov-Gilbert-type upper bounds on number of parity check symbols for codes correcting error patterns mentioned in this section can be obtained similarly as the corresponding bounds for codes correcting random errors of class-weight t or less in Theorem 3.3 and Theorem 3.5 respectively, were found. Therefore, we just state (without proof) the results concerning lower bounds on number of parity-checks as in Theorem 3.7 and results concerning upper bounds on number of parity-checks as Theorem 3.8 given below.

Theorem 3.7: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0,B_1\ldots\ldots, B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q, and non-negative integers a, b, t such that $1 \leq a \leq m-1$, b

$\leq$ n and t $\leq$ (m-1)n, for an (n, k) linear code over Z_q to be able to correct all error patterns of class-weight not exceeding t and

i) in which number of error positions does not exceed b, the number of parity-check symbols required is at least

$$\log_q V_{t,\mathcal{P}_1}^{(n,b)} \qquad \text{... (eq 3.52)}$$

where

$V_{t,\mathcal{P}_1}^{(n,b)}$ is given by (eq 3.40) and (eq 3.39).

ii) with intensity limited by a, i.e., in which none of the error positions has class-weight more than a, the number of parity-check symbols required is at least

$$\log_q V_{t,\mathcal{P}_1}^{(n),a} \qquad \text{... (eq 3.53)}$$

where

$V_{t,\mathcal{P}_1}^{(n),a}$ is given by (eq 3.42) and (eq 3.41)

and iii) with intensity limited by a and having number of error positions not exceeding b, the number of parity-check symbols required is at least

$$\log_q V^{(n,b),a}_{t,\mathcal{P}_1} \qquad \ldots \text{(eq 3.54)}$$

where

$V^{(n,b),a}_{t,\mathcal{P}_1}$ is given by (eq 3.44) and (eq 3.43).

Next, we state the result concerning Varshamov-Gilbert-Sacks-type bounds on number of parity-check symbols in codes correcting error patterns considered in this section.

Theorem 3.8: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, q prime, determining the class metric under consideration and non-negative integers a, b, t such that $1 \le a \le m-1$, $b \le n$ and $t \le (m-1)n$, it is always possible to construct an (n, k) linear code that corrects all error patterns each of which is of class-weight not exceeding d and

i) with number of error positions not exceeding b, if the following inequality holds:

$$V^{(n,b)}_{2d-1,\mathcal{P}_1} \ge q^{n-k},$$

where

$V^{(n,b)}_{t,\mathcal{P}_1}$ is given by (eq 3.40) and (eq 3.39)

ii) with intensity limited by a, if the following inequality holds

$$V^{(n),a}_{2d-1,\mathcal{P}_1} \geq q^{n-k},$$

where

$V^{(n),a}_{t,\mathcal{P}_1}$ is given by (eq 3.42) and (eq 3.41)

and iii) with intensity limited by a and number of error positions not exceeding b, if the following inequality holds

$$V^{(n,b),a}_{2d-1,\mathcal{P}_1} \geq q^{n-k},$$

where

$V^{(n,b),a}_{2d-1,\mathcal{P}_1}$ is given by (eq 3.44) and (eq 3.43)

Remarks: If in Theorem 3.7 and Theorem 3.8, we take n = b and a = (m-1), then all the bounds on number of parity-check symbols obtained in Theorem 3.7 coincide with that obtained in Theorem 3.3 and similarly all the bounds derived in Theorem 3.8 coincide with those obtained in Theorem 3.5.

Corollary 3.5: In the case of Hamming metric, the restriction on number of error positions in error patterns covered in cases (i) of Theorem 3.7 and Theorem 3.8 is redundant in the sense that t (Hamming) errors in an error vector arise out of exactly t nonzero positions in it.

Further, the idea of intensity is irrelevant when metric under consideration is the Hamming metric, as every (nonzero) error position has weight one, i.e., a is always 1.

Thus in the case of Hamming metric, the results derived in Theorem 3.7 and Theorem 3.8 coincide respectively with those of Theorem 4.8 and Theorem 4.7 given of Peterson and Weldon (1972).

It seems that a number of interesting code constructions to correct random errors are possible with reference to the new metrics. Particularly the notion of cyclic codes can possibly be extended with due modifications, to a class of codes which may come out to be constacyclic, (for definition, refer Berlekamp, 1968). The details and complexities of construction and decoding of such codes are yet to be worked out.

CHAPTER IV

BURSTS WITH WEIGHT CONSTRAINTS

4.1 Introduction

4.2 Class Weights of Bursts

4.3 Bounds for Codes Detecting/Correcting Bursts that have a Given Class Weight or Less

CHAPTER IV

BURSTS WITH WEIGHT CONSTRAINTS

4.1 Introduction

In Chapter I we have emphasised that the errors introduced by most of the channels, tend to occur in bursts rather than occurring at random (c.f. Forney, 1971). This leads to the study of burst error-correcting codes in which earlier studies have been conducted by Ambramson (1959), Fire (1959), Farrell and Hopkins (1982), Daniel (1985), Blaum, Farrell and Tilborg (1986, 1988), Abdel-Ghaffar, McElice and Tilborg (1988), Blaum (1990), Zhang and Wolf (1990). When bursts are introduced by impulse noise, as happens in the case of large number of practical channel, the length of burst depends upon the duration of the impulse noise. Also, the number of errors, i.e., the density of errors within a burst clearly depends upon the intensity of the impulse noise. In the case of the behaviour of the channel, either due to impulse noise or otherwise, being such that the density of errors in the bursts introduced by the channel is either too small or too large, employing the usual burst-correcting codes is not quite appropriate for the purposes of efficient transmission over such a channel. One class of codes correcting only those bursts in which only a limited number of positions are disturbed is given by low-density-burst-correcting codes (refer Wyner, 1963).

The problem of the density of errors in a burst in terms of the weight of the burst was considered by Sharma and Dass (1974). They introduced the notion of the burst with the weight constraints and derived Varshamov-Gilbert-type bounds for codes correcting bursts with weight constraints. This idea of bursts with weight constrains prompted the study of similar problems in terms of other metrics. Sharma and Goel (1977) did so in terms of Lee metric.

Chapter IV is devoted to the study of some problems of detecting/correcting bursts with weight constraints with reference to class-metrics. As Hamming and Lee metrics are particular class-metrics, some of the results of Sharma and Dass (1974) and Sharma and Goel (1977) are derived as particular cases of the corresponding results for class-metrics given in this chapter.

As earlier, we shall consider vectors $(a_1, \ldots, a_n)$ of length n where a_i are elements of a finite field Z_q and the class-metric under consideration is determined by a $\mathcal{P}$-Partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q. As the notion of burst will be used very frequently, we repeat its definition below (see Chapter-I).

Definition: A *burst* of length b is a vector whose only nonzero elements are among b successive components, the first and last of which are nonzero (Peterson and Weldon, 1972).

Also we shall need the following definition of a burst with a given class-weight based on the idea of a burst with weight constraints.

Definition: A burst of length b, which has class-weight w as an n-tuple over Z_q, will be called a *burst of length b and class-weight w.*

In the next section of this chapter, we obtain combinatorial results on class-weights of bursts. Theorem 4.1 and Theorem 4.2 determine total class-weights of bursts of length b and of bursts of length b or less respectively. These results will be used in Theorem 4.3 and Theorem 4.4 of this chapter and also in subsequent chapters in deriving bounds on minimum class-distances of codes under study in the thesis. Theorem 4.3 and Theorem 4.4 determine upper bounds on minimum class-weights respectively of a bursts of length b and of a burst of length b or less and thus provide bounds on the random error correcting capabilities of respective codes.

Further, the weight-enumerator of a code contains a good deal of information about the structure of a code, including its minimum distance, the number of code words of each weight, and the probabilities of decoding error and failure.

We have included in Section 4.2 results on class-weight enumerators of all bursts of length b and of length b or less in the space of n-tuples, as these may prove helpful similarly.

The third section of the chapter deals with codes detecting/correcting bursts with class-weight constraints.

4.2 Class-Weight of Bursts

In finding out the total class-weights of burst of length b, we will be making use of the following.

Lemma 4.1: In the space of n-tuples over Z_q, q prime, the total number of bursts of length $b > 1$, that have w nonzero entries , $w \leq b$, is

$$(n-b+1)\binom{b-2}{w-2}(q-1)^{w} \qquad \text{... (eq 4.1)}$$

Proof: There are (n-b+1) possible starting positions for a burst of length b. For each starting position say i^{th}, we should have nonzero field elements in the i^{th} and $(b+i-1)^{th}$ positions. The remaining (w-2) nonzero positions are to be chosen out of (b-2) positions. The proof follows from the fact that each nonzero position may be any of the (q-1) nonzero field elements and the remaining positions are to be zero.

Theorem 4.1: For a given $\mathcal{P}$-partition, $\mathcal{P}_1=\{B_0,B_1,\ldots,B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, q prime, the total class-weight of all bursts of length b in this space, denoted by $W_{b,\mathcal{P}_1}$ is given by

$$W_{1,\mathcal{P}_1} = n.W(\mathcal{P}_1) \qquad \ldots \text{(eq 4.2)}$$

and

$$W_{b,\mathcal{P}_1} = (n-b+1)[b(q-1)+2](q-1)q^{b-3}W(\mathcal{P}_1) \quad \text{for } b > 1 \qquad \ldots \text{(eq 4.3)}$$

where

$$W(\mathcal{P}_1) = \sum_{i=1}^{m-1} i|B_i| .$$

Proof: Let $\underline{u}$ be any burst of length $b \geq 1$ having w nonzero entries $(0 < w \leq b)$. We form a matrix A, the rows of which are all non-zero scalar multiples of $\underline{u}$. Each nonzero element of the ground field Z_q clearly occurs exactly once in each of the w nonzero columns of A. Therefore, the sum of the class-weights of (q-1) n-vectors appearing in the matrix A is

$$w.W(\mathcal{P}_1) \qquad \ldots \text{(eq 4.4)}$$

If b = 1, then w = 1, and hence the sum of the class-weights of (q-1) bursts of length one appearing in A is $W(\mathcal{P}_1)$.

However, since there are n possible starting positions for a bursts of length one, the sum of class-weights of bursts of length one is

$$n.W(\mathcal{P}_1) .$$

In general, from lemma 4.1, the total number of bursts of length b, having w non-zero entries, is

$$(n-b+1)\binom{b-2}{w-2}(q-1)^{w} \quad \text{for } b > 1$$

Let β be a partition of the set of all bursts of length b having w nonzero entries, such that each member set of the partition β consists of (q-1) mutual non-zero scalar multiple bursts. Then number of sets in β is obtained by dividing the expression in (eq 4.1) by (q-1), i.e.,

$$|\beta| = (n-b+1)\binom{b-2}{w-2}(q-1)^{w-1} \qquad \text{... (eq 4.5)}$$

Also, from (eq 4.4), it follows that the sum of the class-weights of bursts in each member set of β is w.W($\mathcal{P}_1$). Therefore, total class-weight of all bursts of length b and having w nonzero entries is given by

$$(n-b+1)\binom{b-2}{w-2}(q-1)^{w-1}\ w.W(\mathcal{P}_1) \qquad \text{... (eq 4.6)}$$

Finally, the total class-weight $W_{b,\mathcal{P}_1}$, of bursts of length b (>1) is obtained by summing (eq 4.6) over w = 2 to w = b, i.e.,

$$W_{b,\mathcal{P}_1} = \sum_{w=2}^{b}(n-b+1)\binom{b-2}{w-2}(q-1)^{w-1}\,w.W(\mathcal{P}_1)$$

$$= (n-b+1)W(\mathcal{P}_1)\sum_{j=0}^{b-2}\binom{b-2}{j}(q-1)^{j+1}(j+2)$$

By substituting w = j+2

$$= (n-b+1)\, W(\mathcal{P}_1)\, \frac{d}{dq}\left[\sum_{j=0}^{b-2}\binom{b-2}{j}(q-1)^{j+2}\right]$$

$$= (n-b+1) W(\mathcal{P}_1) \frac{d}{dq}\left[(q-1)^2\, q^{b-2}\right]$$

$$= (n-b+1) W(\mathcal{P}_1)(q-1)q^{b-3}\left[2q+(q-1)(b-2)\right]$$

$$= (n-b+1)(q-1)q^{b-3}\left[b(q-1)+2\right] W(\mathcal{P}_1)$$

This completes the proof of the Theorem 4.1.

In the next theorem we determine the sum of class-weights of all bursts of length b or less. This is denoted by $W^{T}_{b,\mathcal{P}_1}$.

Theorem 4.2: Given a $\mathcal{P}$-partition $\mathcal{P}_1$ = {B_0, B_1,...,B_{m-1}} of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q; $W^{T}_{b,\mathcal{P}_1}$, the total class-weight of all n-tuples, which are bursts of length b or less is given by

$$W^{T}_{b,\mathcal{P}_1} = \frac{\left[b(n-b+1)q^{b} + \{n-2b(n-b+1)\}q^{b-1} + (b-1)(n-b)q^{b-2}\right]W(\mathcal{P}_1)}{q-1} \quad \text{... (eq 4.7)}$$

Proof: From Theorem 4.1, we have

$$W^{T}_{b,\mathcal{P}_1} = W_{1,\mathcal{P}_1} = W(\mathcal{P}_1) \qquad \text{for } b = 1$$

For b > 1, we have

$$W^{T}_{b,\mathcal{P}_1} = W_{1,\mathcal{P}_1} + \sum_{j=2}^{b} W_{j,\mathcal{P}_1} .$$

Substituting the value of $W_{1,\mathcal{P}_1}$ and $W_{j,\mathcal{P}_1}$ for $j \geq 2$, from Theorem 4.1, we get

$$W^{T}_{b,\mathcal{P}_1} = n.W(\mathcal{P}_1) + \sum_{j=2}^{b}(n-j+1)(q-1)\,\{j(q-1)+2\}q^{j-3}\,W(\mathcal{P}_1)$$

$$= \left[n + 2(n+1)(q-1) \sum_{j=2}^{b} q^{j-3} + (q-1)\,\{(q-1)(n+1)-2\} \sum_{j=2}^{b} jq^{j-3} - (q-1)^2 \sum_{j=2}^{b} j^2 q^{j-3} \right] W(\mathcal{P}_1) \qquad \text{... (eq 4.8)}$$

It follows easily that

$$\sum_{j=2}^{b} q^{j-3} = \frac{1}{q} + \frac{q^{b-2}-1}{q-1} \qquad \text{... (eq 4.9)}$$

$$\sum_{j=2}^{b} j\,q^{j-3} = \frac{bq^{b-2}}{q-1} - \frac{2}{q(q-1)} - \frac{q^{b-2}-1}{(q-1)^2} \qquad \text{... (eq 4.10)}$$

and

$$\sum_{j=2}^{b} j^2 q^{j-3} = \frac{4}{q(q-1)^2} + \frac{2q\left(q^{b-3}-1\right)}{(q-1)^3} + \frac{b^2 q^{b-1} - \left(b^2+2b-1\right)q^{b-2}+1}{(q-1)^2} \qquad \text{... (eq 4.11)}$$

Using (eq 4.9), (eq 4.10) and (eq 4.11) in (eq 4.8) we get

$$W^{T}_{b,\mathcal{P}_1} = \left[n + 2(n+1)(q-1)\left\{\frac{1}{q} + \frac{q^{b-2}-1}{q-1}\right\} + \{(n+1)(q-1)-2\}\left\{bq^{b-2} - \frac{2}{q} - \frac{q^{b-2}-1}{q-1}\right\} - \left\{\frac{4}{q} + \frac{2q\left(q^{b-3}-1\right)}{q-1} + b^2q^{b-1} - \left(b^2+2b-1\right)q^{b-2} + 1\right\} \right]_{W(\mathcal{P}_1)}$$

$$= \frac{b(n-b+1)q^{b} + \{n - 2b(n-b+1)\}q^{b-1} + (b-1)(n-b)q^{b-2}}{q-1}\; W(\mathcal{P}_1)$$

Remarks: That the total class-weight of all n-tuples is

$$nq^{n-1}\, W(\mathcal{P}_1),$$

follows from the result of the previous theorem by putting b=n.

4.2.1 Bounds on Minimum Class-Weight of Bursts:

Next, we derive bounds on the largest minimum class-weight attainable by a burst of length b and a burst of length b or less in the space of n-tuples. The technique is essentially similar to that of finding out bound on minimum distance by taking average given by Plotkin (1960).

Theorem 4.3: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, the minimum class-weight of a bursts of length $b > 1$ in the space of n-tuples is at most equal to

$$\left[\frac{b}{q} + \frac{2}{q(q-1)}\right] W(\mathcal{P}_1) \qquad \ldots \text{ (eq 4.12)}$$

Proof: It easily follows that the number of bursts of length b in the space of n-tuples with symbols taken from the field of q elements is

$$(n - b + 1)\ (q - 1)^2 . q^{b-2}$$

Also, from Theorem 4.1, their total class-weight, i.e., sum of class-weights of bursts of length b is

$$(n - b + 1)\,[b(q-1) + 2](q-1)q^{b-3}\, W(\mathcal{P}_1) .$$

Since minimum never exceeds the average, an upper bound on minimum class-weight of a burst of length b is given by

$$\frac{(n - b + 1)[b(q-1) + 2](q-1)q^{b-3}\, W(\mathcal{P}_1)}{(n - b + 1)(q-1)^2\, q^{b-2}},$$

i.e.,
$$\frac{b(q-1) + 2}{(q-1)q}\, W(\mathcal{P}_1) = \left[b + \frac{2}{q-1}\right] \frac{W(\mathcal{P}_1)}{q}$$

It is interesting to note that this bound is independent of n, the length of the words, a property which is true for the classical Plotkin bounds (refer Peterson and Weldon, 1972).

Next theorem provides an upper bound on minimum class weight of a burst of length b or less.

Theorem 4.4: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, the minimum class-weight of a burst of length b or less in the space of all n-tuples is at most

$$\frac{W(\mathcal{P}_1)}{q-1} \; \frac{b(n-b+1)\,q^{b} + [n-2b(n-b+1)\,]q^{b-1} + (b-1)(n-b)q^{b-2}}{[(n-b+1)\,(q-1)+1]q^{b-1} - 1}$$

... (eq 4.13)

Proof: The number of bursts of length b in the space of n-tuples over Z_q is given by

$$n(q-1) \qquad \text{for } b = 1$$

and $$(q-1)^2\, q^{b-2}(n-b+1) \qquad \text{for } b \geq 2$$

Therefore, the number of bursts of length b or less in the space of n-tuples over Z_q is given by

$$n(q-1) + (q-1)^2 \sum_{i=2}^{b} (n-i+1)\, q^{i-2}\,,$$

i.e., $$q^{b-1}\;[(n-b+1)(q-1)+1]-1$$

Also, from Theorem 4.2, the total class-weight of all bursts of length b or less is equal to

$$\frac{W(\mathcal{P}_1)}{q-1}\left[b(n-b+1)q^{b} + \{n-2b(n-b+1)\}q^{b-1} + (b-1)(n-b)q^{b-2}\right]$$

The result then follows from the argument that the minimum cannot exceed the average.

4.2.2 Generating Functioning for $W_{b,\mathcal{P}_1}$ and $W^{T}_{b,\mathcal{P}_1}$

Weight generating functioning for linear codes have been helpful in enumerating code words of a given weight. Therefore, it is interesting to evaluate generating functions of $W_{b,\mathcal{P}_1}$ and $W^{T}_{b,\mathcal{P}_1}$. We give these in the following two theorems. These may be helpful for a similar study of burst-error detecting or correcting codes.

Theorem 4.5: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots., B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, q prime and $n \geq b \geq 1$, $W_{b,\mathcal{P}_1}$, the total class-weight of bursts of length b, is the coefficient of x^b in

$$nW(\mathcal{P}_1)x + \left[n(q+1)qx^2 - \{n(3q+1)-2\}x + 2(n-1)\right]x^2(q-1)W(\mathcal{P}_1)(1-qx)$$

where $W(\mathcal{P}_1) = \sum\limits_{i=1}^{m-1} |B_i|$ ... (eq 4.14)

Proof: If f(x) is the generating function of $W_{b,\mathcal{P}_1}$, then

$$f(x) = \sum_{i=1}^{n} W_{i,\mathcal{P}_1} x^i = W_{1,\mathcal{P}_1}.x + \sum_{i=2}^{n} W_{i,\mathcal{P}_1}.x^i \qquad \text{... (eq 4.15)}$$

$$= nW(\mathcal{P}_1)x + \sum_{i=2}^{n} (n-i+1)\left[i(q-1)+2\right](q-1)W(\mathcal{P}_1)q^{i-3}x^i$$

from (eq 4.2) and (eq 4.3)

$$= nW(\mathcal{P}_1)x \; + \; (q-1)\; W(\mathcal{P}_1)\, x^3 \;\sum_{i=2}^{n}\Big[-(q-1)i^2 + \{(n+1)(q-1)-2\}i$$

$$+\, 2(n+1)\Big](q.x)^{i-3}$$

$$= n\,W(\mathcal{P}_1) - (q-1)^2\; W(\mathcal{P}_1)\, x^3 . \sum_{i=2}^{n} i^2\,(q.x)^{i-3}$$

$$+ (q-1)\; W(\mathcal{P}_1)\big[(n+1)(q-1)-2\big]x^3 \;\sum_{i=2}^{n} i(q.x)^{i-3}$$

$$+\, 2(n+1)(q-1)\, W(\mathcal{P}_1)x^3 \;\sum_{i=2}^{n}(q.x)^{i-3}$$

$$= nW(\mathcal{P}_1)x - (q-1)^2\, W(\mathcal{P}_1)x^3\left[\frac{4}{qx(qx-1)^2} + \frac{2qx(q^{n-3}x^{n-3}-1)}{(qx-1)^3}\right.$$

$$\left. + \;\frac{n^2q^{n-1}x^{n-1} - (n^2+2n-1)q^{n-2}x^{n-2} + 1)}{(qx-1)^2}\right]$$

$$+\,(q-1)w(\mathcal{P}_1)\big[(n+1)(q-1)-2\big]x^3\left[\frac{n(qx)^{n-2}}{qx-1} - \frac{2}{qx(qx-1)} - \frac{(qx)^{n-2}-1}{(qx-1)^2}\right]$$

$$+\,2(n+1)\,(q-1)\;W(\mathcal{P}_1)x^3\left[\frac{1}{qx} + \frac{(qx)^{n-2}-1}{qx-1}\right],$$

summing the series as in Theorem 4.2.

After simplification, we get

$$f(x) = nW(\mathcal{P}_1)x + (q-1)W(\mathcal{P}_1)x^2 \left[n(q+1)qx^2 - \{n(3q+1)-2\}x \right.$$
$$\left. + 2(n-1)\right](1-qx)^{-3} - (q-1)W(\mathcal{P}_1)q^{n-1}\, x^{n+2}\, [\{n(q-1)+2\}qx$$
$$-\{(n(q-1)+2q\}](1-qx)^{-3}$$

... (eq 4.16)

The last term in expression (eq 4.16) contains terms involving x^{n+2} and of higher orders. Since the length of a burst cannot exceed n, therefore, this term may be dropped altogether. Then we obtain the generating function of $W_{b,\mathcal{P}_1}$ as stated in (eq 4.14).

Next, we obtain generating function for $W^T_{b,\mathcal{P}_1}$.

Theorem 4.6: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric in the space of n-tuples over Z_q, q prime, and $n \geq b \geq 1$; $W^T_{b,\mathcal{P}_1}$, the sum of class-weights of bursts having lengths less than or equal to b, is the coefficient of x^b in

$$W(\mathcal{P}_1) \ x \ \left[nqx^2 - \{(n+2)(q-1)+2n\}x + n\right](1-qx)^{-3} \qquad \text{... (eq 4.17)}$$

Proof: The expression having $W^T_{b,\mathcal{P}_1}$ as the coefficient of x^b in general can be written as

$$\sum_{i=1}^{n} W^T_{i,\mathcal{P}_1} x^i$$
$$= \frac{W(\mathcal{P}_1)}{(q-1)} \sum_{i=1}^{n} \left[i(n-i+1)q^i + \{n-2i(n-i+1)\}q^{i-1} + (i-1)(n-i)q^{i-2}\right]x^i$$

(using Theorem 4.2)

$$= \frac{W(\mathcal{P}_1)}{(q-1)} \sum_{i=1}^{n} \left[- i^2\left(q^2 - 2q + 1\right) + i\left\{(n+1)q^2 - 2(n+1)q + (n+1)\right\} + n(q-1)\right]q^{i-2}x^i$$

$$= -W(\mathcal{P}_1)(q-1)x^2 \sum_{i=1}^{n} i^2 q^{i-2}x^{i-2} + (n+1)(q-1)W(\mathcal{P}_1)x^2 \sum_{i=1}^{n} i q^{i-2}x^{i-2}$$

$$+ n\, W(\mathcal{P}_1)x^2 \sum_{i=1}^{n} q^{i-2}\, x^{i-2}$$

$$= -W(\mathcal{P}_1)(q-1)x^2 \left[\frac{1}{qx} + \frac{4}{(qx-1)^2} + \frac{2q^2x^2(q^{n-3}x^{n-3} - 1)}{(qx-1)^3} + \frac{n^2q^nx^n - \left(n^2 + 2n - 1\right)q^{n-1}x^{n-1} + qx}{(qx-1)^2} \right]$$

$$+ (n+1)(q-1)W(\mathcal{P}_1)x^2 \left[\frac{1}{qx} + \frac{nq^{n-1}x^{n-1}}{qx - 1} - \frac{2}{qx - 1} - \frac{q^{n-1}x^{n-1} - qx}{(qx - 1)^2} \right]$$

$$+ n\ W(\mathcal{P}_1)x^2 \left[\frac{1}{qx} + 1 + \frac{q^{n-1}x^{n-1} - qx}{qx - 1} \right]$$

$$= W(\mathcal{P}_1)q^{n-1}\, x^{n+1}\left[- nq^3x^2 + \{(n + 2)\,(q - 1) + 2n\}qx - n\right](1 - qx)^{-3}$$

$$+ W(\mathcal{P}_1)x\left[nqx^2 - \{(n + 2)\,(q - 1) + 2n\}x + n\right](1 - qx)^{-3}$$

(after simplification)

Now, the first term on the right hand side of the Preceding expression contains terms involving x^{n+1} and of higher orders and therefore can be dropped altogether as in Theorem 4.5.

Thus, the generating function of $W^{T}_{b,\mathcal{P}_1}$ is as stated in (eq 4.17).

Remarks: Particular cases of all the results derived in Section 4.2, may be obtained for Hamming metric by taking $\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\}$ where $B_1 = \{1,2,\ldots,q-1\}$ and hence

$$W(\mathcal{P}_1) = W(\mathcal{P}_H) = (q-1)$$

Thus, the results on weights of bursts and weight-enumerators given in Dass (1974), may be derived as particular cases of the corresponding results of this section.

Again, if we take

$$\mathcal{P}_1 = \mathcal{P}_L = \left\{B_0, B_1, \ldots B_{\frac{q-1}{2}}\right\} \qquad \text{(for q odd prime)}$$

where $\qquad B_i = \{i, q-i\}$

then $\qquad W(\mathcal{P}_1) = W(\mathcal{P}_L) = \dfrac{q^2-1}{4}$

Replacing $W(\mathcal{P}_1)$ by $\dfrac{q^2-1}{4}$ in all the results of this section, we obtain corresponding results on Lee-weights of bursts and Lee-weight enumerators of bursts.

4.3 Bounds for Codes detecting /Correcting Bursts that have a Given Class-Weight or Less.

We have pointed out in Section 4.1 that when a channel under consideration introduces bursts in messages, then either due to intensity of impulse noise or otherwise, the number of digits within a bursts and hence the class-weight of a burst may not exceed a given number. The usual burst-correcting codes which do not take into consideration the intensity limitation, if employed, will have more parity-check digits than are required, effecting adversely the efficiency of the transmission. Thus a study of bursts detecting/correcting codes is required keeping in view that detection/correction of all bursts of a specified length or less, is not required. Such a study can be made by imposing a suitable class-weight constraint over detectable or correctable bursts. The development of such codes would result in the saving of parity-check digits and reducing thereby the redundancy of a code suitable for a specific purpose.

We begin with the problem of detecting errors, which are in the form of bursts of lengths b or less and of class-weight w or less. The study is then extended to the correction of such errors. We derive lower and upper bounds on the necessary and sufficient number of check digits required for such codes. Reiger (1960), Fire (1959) and others have found similar bounds for bursts-error (without weight constraints) detection and correction. Some of these results are shown to be particular cases of the results derived in this section.

We first consider codes having no bursts of length b or less that is of class-weight w or less ($w \leq (m-1)b$) as a code word. Such a code may have a burst of length b or less as a code word but class-weight of that burst must then be greater than w. Similarly, it may have code words of class-weight less than or equal to w, which are then the bursts of length greater than b.

Theorem 4.7: Given a $\mathcal{P}$-partition $\mathcal{P}_1$ = $\{B_0,B_1,\dots,B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q, an (n, k) linear code that has no non-zero burst of length b or less that is of class-weight w or less ($w \leq (m-1)b$) as a code word, must satisfy

$$(n-k)>\log_q V^{(b)}_{\lfloor w/2 \rfloor,\mathcal{P}_1} \qquad \text{... (eq 4.18)}$$

where $V^{(n)}_{t,\mathcal{P}_1}$ is as given by (3.19) and b < n.

Proof: The proof given here is a modification of the one given in Theorem 4.6 (Peterson, 1961).

Since a burst of length b or less that has class-weight w or less is not a code word, therefore no two n-vectors of class-weight $\lfloor w/2 \rfloor$ or less with zeros in positions from (b+1)th to nth can be in the same coset, because otherwise there difference which must be a burst of length b or less that is a burst of class-weight w or less will be a code word.

The number of vectors of class-weight $\lfloor w/2 \rfloor$ or less with zeros in positions numbering (b+1) to n is equal to the number of b-tuples over z_q with class-weight $\lfloor w/2 \rfloor$ or less, i.e. $V^{(b)}_{\lfloor w/2 \rfloor,\mathcal{P}_1}$.

Since there must be at least this number of cosets and the total number of cosets is exactly q^{n-k}, we have

$$q^{n-k} \geq V^{('b)}_{\lfloor w/2 \rfloor,\mathcal{P}_1} \qquad \text{... (eq 4.19)}$$

Here we have considered those bursts which have last nonzero entry before (b+1)th position in the vector, and in case b < n, there are n-vectors which are bursts of length b or less and have their last nonzero entry in either (b+1)th position or after (b+1)th position, therefore strict inequality should be taken in expression (eq 4.19) i.e., the following should hold.

$$q^{n-k} > V^{(b)}_{\lfloor w/2 \rfloor, \mathcal{P}_1} \qquad \text{... (eq 4.20)}$$

Taking logarithm or both sides we get the required result.

Corollary 4.1: By substituting m = 2 and $\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\}$, $B_1=\{1, \ldots, q-1\}$ in Theorem 4.7 we get the corresponding result for Hamming metric which is similar to Theorem 4.1 of Dass (1974).

Again, if we take m-1 = (q-1)/2 and $\mathcal{P}_1 = \mathcal{P}_L = \{B_0, B_1, \ldots, B_{(q-1)/2}\}$ for q odd-prime, where $B_i = \{i, q-i\}$ in Theorem 4.7, we get the corresponding result for Lee metric in the form of the following.

Corollary 4.2: An (n, k) linear code over, Z_q, q an odd prime, that has no non-zero burst of length b or less that is of Lee-weight w or less ($w \le \frac{(q-1)}{2}.b$) as a code word, must satisfy

$$(n-k) > \log_q V^{(b)}_{\lfloor w/2 \rfloor, \mathcal{P}_L},$$

where

$V^{(b)}_{t,\mathcal{P}_L}$ denotes the b-dimensional sphere of Lee-radius t. The value of $V^{(b)}_{t,\mathcal{P}_L}$ can be obtained from (eq 3.19).

Next, we obtain an upper bound on the number of parity-check symbols for codes considered in Theorem 4.7. This bound assures the existence of a Linear code that can detect all error patterns which are bursts of length b or less and have class-weight w or less. The proof will be essentially on the lines of one given by Sacks (1958) for Varshamov-Gilbert bound for random error-correcting codes.

Theorem 4.8: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots., B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q and two positive integers w and b such that $w \leq (m-1)b$; a sufficient condition that there exists an (n, k) linear code that has no nonzero burst of length b or less that has class-weight w or less as a code word is:

$$V^{(b-1)}_{w-1,\mathcal{P}_1} < q^{n-k} \qquad \ldots \text{(eq 4.21)}$$

Proof: To show that existence of such a code, we examine the existence of a suitable (n-k)×n parity-check matrix H for the desired code.

Choose a nonzero (n-k)-tuple as the first column of the parity-check matrix H (c.f. Peterson and Weldon (1972), Theorem 4.7). Subsequent columns are added such that after having selected (j-1) columns $h_1, h_2, \ldots, h_{j-1}$, a column h_j is added provided that it is not a linear combination of class-weight (w-1) or less of the columns from amongst immediately preceding (b-1) columns. This restriction ensures that no burst of length b or less which is of class-weight w or less can be a code word.

In other words, a column h_j is to be added provided that it is not a linear combination of class-weight (w-1) or less of the column from amongst $h_{j-b+1} : h_{j-b+2}, \ldots., h_{j-1}$.

In the worst case, all the linear combinations of class-weight (w-1) or less of column from amongst the previous (b-1) columns may be distinct. There are at most $V_{w-1,\mathcal{P}}^{(b-1)}-1$ distinct such linear combination.

If this is less than the total number of nonzero (n-k)-tuples then there is certainly one more column that can be added to the matrix. That is, if

$$V_{w-1,\mathcal{P}}^{(b-1)}-1<q^{n-k}-1, \qquad \text{... (eq 4.22)}$$

jth column can be added to the matrix.

But for an (n, k) linear code to exist, relation (eq 4.22) should hold for j=n, so that it is always possible to add nth column to the matrix.

As expression (eq 4.22) is independent of j, therefore we can add columns as long as we wish for given b, w and k.

But to construct a code of specified length n, we shall stop after, adding n column appropriately.

Therefore, an (n, k) linear code that has no nonzero burst of length b or less that has class-weight w or less as a code word exists satisfying (eq 4.21).

Remarks: If we set b = n, we see that the bound obtained in (eq 4.21) immediately reduces to Varshamov-Gilbert-Sacks bound for a code having minimum class - weight at least (w+1).

In the particular case of Hamming metric, the Theorem 4.8 reduces to Theorem 4.2 of Dass (1974), an equivalent version of which is stated as Corollary 4.3 given below. For this we substitute m=2 and $\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\}$, $B_1 = \{1,\ldots,q-1\}$ in Theorem 4.8 and get the following.

Corollary 4.3: Given two positive integers w and b such that $w \leq b$, a sufficient condition that there exists an (n, k) linear code that has no non-zero burst of length b or less that is of (Hamming) weight w or less is

$$V_{w-1,\mathcal{P}_H}^{(b-1)} < q^{n-k}$$

where value of $V_{t,\mathcal{P}_H}^{(n)}$ is given from (eq 3.22).

Further by taking m-1 = (q-1)/2 and
$\mathcal{P}_L = \mathcal{P}_L = \{B_0, B_1, \ldots, B_{(q-1)/2}\}$ $B_i = \{i, q-i\}$, i=1,2,...,(q-1)/2
in Theorem 4.8, the result of Theorem 4.8 can be stated as the Corollary 4.4.

Corollary 4.4: Given two positive integers w and b s.t. $w \leq \frac{(q-1)}{2} b$, q-odd prime, a sufficient condition that there exists an (n, k) linear code that has no burst of length b or less that is of Lee-weight w or less is

$$V_{w-1,\mathcal{P}_L}^{(b-1)} < q^{n-k},$$

where value of $V_{t,\mathcal{P}_L}^{(n)}$ is given by (eq 3.25).

Corollary 4.5: The result obtained above in Theorem 4.8, holds for $w \le (m-1)b$. If we take $w = (m-1)b$, i.e., if w coincides with the maximum possible attainable class-weight in a burst of length b, the weight criterion imposed over the burst becomes redundant and the bound takes the from

$$q^{n-k} > V^{(b-1)}_{(m-1)(b-1),\mathcal{P}_1}$$

$$= q^{b-1}$$

which on taking logarithm of both sides gives

$$n-k > b-1$$

$$n-k \ge b.$$

This leads to the existence of an (n, k) linear code that has no burst of length b or less as a code word with just b parity-checks. This coincides with the result of Theorem 4.7 of Peterson (1961) wherein it has been shown that b parity-checks are sufficient to detect any burst of length b or less.

In determining the bound of Theorem 4.8, we have tried to formulate the result for fixed value of n, k, w and b. It may be desired to obtain the maximum value of b for a fixed number of parity-checks and fixed values of w and n. If this is taken up as the basis of formulation of the problem, then we may alternatively state the result in the following form.

Theorem 4.9: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, q prime, and two positive integers w and b_1 such that $w \leq (m-1)b_1$, it is always possible to construct an (n, k) linear code that has no nonzero burst of length b_1 or less which is of class-weight w or less as a code word for which the inequality.

$$V_{w-1,\mathcal{P}_1}^{(b_1)} \geq q^{n-k} \qquad \text{... (eq 4.23)}$$

holds, where b_1 is the smallest positive integer satisfying this inequality.

Proof: In the proof of Theorem 4.8, let b_1 be the largest value of b for which inequality (eq 4.21) holds.

Then for $b = b_1 + 1$ the inequality (eq 4.21) gets reversed and we get inequality (eq 4.23).

Remarks: Particular cases of the above theorem for Hamming and Lee metrics can be obtained in the similar way as the particular cases of Theorem 4.7 and Theorem 4.8 have been obtained earlier.

Next, we derive bounds for linear codes capable of correcting all bursts of length b or less that are of class-weight w or less.

In the next theorem we obtain a lower bound on the necessary number of check digits for the existence of such a code. This generalizes results due to Fire (1959) and Sharma and Dass (1974).

First, we give a Lemma, which will be used in obtaining the required bounds.

Lemma 4.2: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, N_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, q prime, the total number of bursts of length b (>1) that are of class-weight w or less $2 \le w \le (m-1)b$, in the space of all n-tup1

$$(n-b+1)\sum_{i,j} |B_i||B_j|\, V^{(b-2)}_{w-i-j,\mathcal{P}_1} \quad , \qquad \text{for } b \ge 2 \qquad \text{... (eq 4.24)}$$

where summation runs over i and j taking values from 1 to min {m-1, w-1} and $|B_i|$ denotes number of elements in class B_i of $\mathcal{P}_1$.

Proof: Any burst of length b has (n-b+1) starting positions in an n-tuple space. Further for each starting position say sth we should have sth and (s-b-1)th position as nonzero. If nonzero entries of class-weight say i and j occupy sth and (s+b-1)th positions respectively, then

$$1 < i \le \min\{m-1, w-1\} \text{ and } 1 \le j \le \min\{m-1, w-1\}$$

and the number of such choices in sth and (s+b-1)th positions is

$$|B_i| \; |B_j| \qquad \text{... (eq 4.25)}$$

Also, then the sum of class-weights of entries in positions numbering (s+1),...,(s+b-2) should not exceed w-i-j. Hence the number of choices for entries in (s+1)th .... (s+b-2)th positions is

$$V^{(b-2)}_{w-i-j,\mathcal{P}_1} \qquad \text{... (eq 4.26)}$$

Summing the product of expressions in (eq 4.25) and (eq 4.26) over i and j and multiplying the resultant number with (n-b+1) we get the required number.

Remarks: In the particular case of Hamming metric

$$\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\} \ , \quad B_1 = \{1, \ldots, (q-1)\} \qquad \text{and}$$

$$|B_i| = |B_j| = |B_1| = q-1 \qquad \text{and} \qquad i = j = 1.$$

Therefore, by substituting these values in (eq 4.24), the number of bursts of length b that are of weight w or less is given by

$$(n-b+1)(q-1)^2 \ V^{(b-2)}_{w-2,\mathcal{P}_H}, \qquad \text{... (eq 4.27)}$$

Also, in the case of Lee-metric, for q odd prime,

$$\mathcal{P}_1 = \mathcal{P}_L = \{B_0, B_1, \ldots., B_{(q-1)/2}\} \quad \text{with } B_i = \{i, q-i\}.$$

So that $|B_i| = |B_j| = 2$ for all i and j.

Therefore, the number of bursts of length b that have Lee-weight w or less is given by

$$4(n-b+1) \sum_{i=1}^{\min\left\{\frac{q-1}{2}, w-1\right\}} \ \sum_{j=1}^{\min\left\{\frac{q-1}{2}, w-1\right\}} V^{(b-2)}_{w-i-j,\mathcal{P}_L}, \qquad \text{... (eq 4.28)}$$

where $V^{(n)}_{t,\mathcal{P}_L}$ is given by (eq 3.25).

Theorem 4.10: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q, the number of parity-check symbols in an (n, k) linear code that corrects all bursts of length b or less that are of class-weight w or less $2 \leq w \leq (m-1)b$, is at least

$$\log_q\left[1+n\sum_{i=1}^{\min\{w,m-1\}}|B_i| + \sum_{s=2}^{b}(n-s+1)\sum_{i=1}^{\min\{w-1,m-1\}}\sum_{j=1}^{\min\{w-1,m-1\}}|B_i||B_j|\,V^{(s-2)}_{w-i-j,\mathcal{P}_1}\right] \quad \ldots \text{(eq 4.29)}$$

where $|B_i|$ denotes the number of elements in the class B_i of $\mathcal{P}_1$ and $V^{(n)}_{t,\mathcal{P}_1}$ is given by (eq 3.19) and (eq 3.20).

Proof: Since the code is capable of correcting all bursts of length b or less that are of class-weight w or less, therefore all such error patterns should be in different cosets.

The number of bursts of length one that are of class-weight w or less in the space of n-tuple is given by

$$n\sum_{i=1}^{\min\{w,m-1\}}|B_i|$$

Also, using Lemma 4.2, the number of bursts of length b or less ($b \geq 2$) that are of class-weight w or less is given by

$$\sum_{s=2}^{b}(n-s+1)\sum_{i=1}^{\min\{w-1,m-1\}}\sum_{j=1}^{\min\{w-1,m-1\}}|B_i||B_j|\,V^{(s-2)}_{w-i-j,\mathcal{P}_1}$$

Thus, the total number of error-patterns, i.e., bursts of length b or less that are of class-weight w or less is

$$1+n\sum_{i=1}^{\min\{w,m-1\}}|B_i|$$

$$+\sum_{s=2}^{b}(n-s+1)\sum_{1\le i,j\le \min\{w-1,m-1\}}|B_i||B_j|\,V^{(s-2)}_{w-i-j,\mathcal{P}_1} \qquad \text{... (eq 4.30)}$$

including the all zero n-tuple.

For the possibility of the code being able to correct these numbers of error - patterns, there should be at least so many cosets, whose total number in an (n, k) linear code is q^{n-k}.

In other words, we must have

$$q^{n-k} \;\ge\; \text{expression in (eq 4.30)}$$

The theorem now follows by taking logarithm of both the sides.

In the particular case of Hamming metric, we have.

Corollary 4.6: Given two positive integers w and b such that $2 \le w \le b$, the number of parity-check symbols in an (n, k) linear code over Z_q, q prime, that corrects all bursts of length b or less that are of weight (Hamming) w or less, is at least

$$\log_q\left[1 + n(q-1) + (q-1)^2\sum_{s=2}^{b}(n-s+1)\,V^{(s-2)}_{w-2,\mathcal{P}_H}\right] \qquad \text{... (eq 4.31)}$$

Proof: Hamming metric is obtained by the particular $\mathcal{P}$-partition $\mathcal{P}_H = \{B_0,B_1\}$, $B_1 = \{1,\ldots,q-1\}$ of Z_q. As in this case

$$m-1=1 \text{ and } w \ge 2 \text{ (given)}$$

Therefore,

$$\min\{w, m-1\} = \min\{w-1, m-1\} = 1$$

Also

$$\sum_{i=1} |B_i| = \sum_{j=1} |B_j| = q-1$$

Substituting these values in (eq 4.29), we get (eq 4.31). Hence the corollary follows.

Also, in the case of Lee metric, we have

Corollary 4.7: Given two positive integers w and b such that $2 \le w \le \frac{(q-1)}{2} b$, the number of parity-check symbols in an (n, k) linear code over z_q, q odd prime, that corrects all bursts of length b or less that are of Lee-weight w or less, is at least

$$\log_q \left[1 + 2n.\min\left\{ w, \frac{(q-1)}{2} \right\} + 4\sum_{s=2}^{b} (n-s+1) \sum_{i=2}^{\min\{2(w-1),(q-1)\}} V_{w-i,\mathcal{P}_L}^{(s-2)} \right] \text{... (eq 4.32)}$$

Proof: Lee metric is obtained by the $\mathcal{P}$-partition

$$\mathcal{P}_L = \{B_0, B_1, \ldots, B_{(q-1)/2}\}$$

where $B_i = \{i, q-i\}$ for i = 1,...,(q-1)/2.

Therefore, in this case m-1 = (q-1)/2 and $|B_i|$ =2 for all i.

Substituting these values in (eq 4.29) we get (eq 4.32) and hence Corollary 4.7 follows.

Corollary 4.8: The result in Theorem 4.10 holds for $w \leq (m-1)b$. If we take $w = (m-1)b$, then the weight constraint over burst stands dropped, because no burst of length b or less can have class-weight more than $(m-1)b$.

Also $\min\{(m-1)b, (m-1)\} = m-1$

and as $s \leq b,\ i \leq m-1,\ j \leq m-1,$ (s, i and j occurring in eq 4.32).

We have $b(m-1) - i - j \geq (s-2)(m-1)$

Therefore,

$$V^{(s-2)}_{w-i-j,\mathcal{P}_1} = V^{(s-2)}_{b(m-1)-i-j,\mathcal{P}_1} = V^{(s-2)}_{(s-2)(m-1),\mathcal{P}_1} \quad \text{(follows from eq 3.21)}$$

$$= q^{s-2} \qquad \text{(follows from eq 3.21)}$$

substituting these values in expression (eq 4.30) we get

$$1+n\sum_{i=1}^{m-1}|B_i| + \sum_{s=2}^{b}(n-s+1)\,q^{s-2}\sum_{i=1}^{m-1}\sum_{j=1}^{m-1}|B_i|\,|B_j|$$

But $\sum_{i=1}^{m-1}|B_i| = q-1$ and $\sum_{i=1}^{m-1}\sum_{j=1}^{m-1}|B_i|\,|B_j| = \left(\sum_{i=1}^{m-1}|B_i|\right)\left(\sum_{j=1}^{m-1}|B_j|\right)$

$$= (q-1)^2$$

Therefore expression in (eq 4.30) is equal to

$$1+n(q-1)+(q-1)^2\sum_{s=2}^{b}(n-s+1)q^{s-2} \qquad \text{... (eq 4.33)}$$

Using the two identities

$$\sum_{i=0}^{n} x^{i} = \frac{1-x^{n+1}}{1-x}$$

and $$\sum_{i=0}^{n} x^{i} = \frac{d}{dx}\left(\frac{1-x^{n+1}}{1-x}\right)$$

Substituting these values in (eq 4.33) we get expression in (eq 4.30) is equal to

$$q^{b-1}[(q-1)(n-b+1)+1] \qquad \text{(c.f. Peterson and Weldon, 1972)}$$

and the bound obtained in expression (eq 4.29) reduces to

$$n-1 \geq (b-1) + \log_q[(q-1)(n-b+1)+1]$$

This coincides with the result of Theorem 4.16, Peterson and Weldon (1972), which for the binary case was proved by Fire (1959).

Next, for b = n, the bound in (eq 4.29) gives a necessary condition for a linear code that corrects all random errors of class-weight w or less (c.f. sphere-packing-type bound).

An alternative expression for the number of bursts of length b that are of class-weight may be obtained by different combinatorial considerations of such bursts. This we take up in Lemma 4.2'.

Lemma 4.2': Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q that determines the class-metric under consideration in the space of n-tuples over Z_q, q prime, the number of bursts of length b ≥ 1, that are of class-weight w or less is given by

$$\sum_{j=1}^{w}(n - b + 1)\left\{A_{j,\mathcal{P}_1}^{(b)} - 2A_{j,\mathcal{P}_1}^{(b-1)} + A_{j,\mathcal{P}_1}^{(b-2)}\right\} \qquad \ldots \text{(eq 4.34)}$$

where value of $A_{t,\mathcal{P}_1}^{(n)}$ is given by (3.18) and (3.20).

Proof: Any burst of length b has (n-b+1) starting positions in an n-tuple space. For each starting position say, ith, $A_{j,\mathcal{P}_1}^{(b)}$ gives the number of those b-tuples, extending from ith to (i+b-1)th positions, which are of class weight j. But for a burst of length b starting from ith position, we should have ith and (i+b-1)th positions as nonzero. Therefore, the number of bursts of length b that are of class-weight j and starting from ith position is

$$A_{j,\mathcal{P}_1}^{(b)} - 2A_{j,\mathcal{P}_1}^{(b-1)} + A_{j,\mathcal{P}_1}^{(b-2)} \qquad \ldots \text{(eq 4.35)}$$

Summing the expression in (eq 4.35) over j varying from 1 to w, the number of bursts of length b that are of class-weight w or less is

$$\sum_{j=1}^{w}(n - b + 1)\left\{A_{j,\mathcal{P}_1}^{(b)} - 2A_{j,\mathcal{P}_1}^{(b-1)} + A_{j,\mathcal{P}_1}^{(b-2)}\right\}$$

In view of the Lemma 4.2', Theorem 4.10 may be alternatively stated as

Theorem 4.10': Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q determining the class-metric under consideration in the space of n-tuples over Z_q, q prime, the number of parity-check symbol in an (n, k) linear code that corrects all bursts of length b or less that are of class weight w or less, $1 \leq w \leq (m-1)b$ is at least

$$\log_q \left[1 + \sum_{i=1}^{b} \sum_{j=1}^{w} (n-i+1) \left\{ A^{(i)}_{j,\mathcal{P}_1} - 2A^{(i-1)}_{j,\mathcal{P}_1} + A^{(i-2)}_{j,\mathcal{P}_1} \right\} \right] \quad \text{... (eq 4.36)}$$

The proof of the theorem follows from Theorem 4.10 and Lemma 4.2'.

We now obtain an upper bound on the sufficient number of parity-checks for codes considered in Theorem 4.10. This bound ensures the existence of a linear code that can correct all bursts of length b or less that are of class-weight w or less.

Theorem 4.11: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q that determines the class-metric under consideration in the space of n-tuples over Z_q, q prime, and two positive integers w and b such that $2b \leq n$ and $w \leq (m-1)b$, a sufficient condition that there exists an (n, k) linear code that corrects all bursts of length b or less that are of class-weight w or less, is given by the inequality

$$q^{n-k} > V^{(b-1)}_{w-1,\mathcal{P}_1} \left[1 + \sum_{i=1}^{b} \sum_{j=1}^{w} (n-b-i+1) \left\{ A^{(i)}_{j,\mathcal{P}_1} - 2A^{(i-1)}_{j,\mathcal{P}_1} + A^{(i-2)}_{j,\mathcal{P}_1} \right\} \right]$$

$$+ V^{(b-1)}_{2w-1,w-1,\mathcal{P}_1}$$

$$+ \sum_{k=1}^{b-1} \sum_{l=1}^{m-1} \sum_{r_{1_l}, r_{2_l}, r_{3_l}} |B_l| A^{(b-k-1)}_{r_{1_l},\mathcal{P}_1} A^{(k)}_{r_{2_l},\mathcal{P}_1} A^{(b-k-1)}_{r_{3_l},\mathcal{P}_1} \quad \text{... (eq 4.37)}$$

where

$$0 \le r_{1_l} \le w - l - 1, \quad 1 \le r_{2_l} \le 2w - l - 1, \quad 0 \le r_{3_l} \le w - 1$$

$$r_{2_l} + r_{3_l} \ge w, \qquad r_{1_l} + r_{2_l} + r_{3_l} \le 2w - l - 1$$

and $V^{(n)}_{t,\mathcal{P}_1}, A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t_1,t_2,\mathcal{P}_1}$ are given by (eq 3.19), (eq 3.18) and (eq 3.26).

Proof: We establish the result by examining the existence of an appropriate r×n parity-check matrix H for the desired code with r parity - checks symbols.

For the code to be able to correct all bursts of length b or less that are of class-weight w or less, no code word in it should be the sum of two bursts of length b or less that are of class-weight w or less. Hence the sum of two linear combinations, each of class-weight w or less of the columns of H from amongst b consecutive columns of H should be non-null. Select a nonzero r-tuple as the first column of the parity-check matrix H, (c.f. Peterson and Weldon, 1972, Theorem 4.7).

Subsequent columns are added to H such that after having selected (j-1) columns $h_1, h_2, \ldots, h_{j-1}$, a column h_j is added provided that it is not a sum of a linear combination of class-weight (w-1) or less of columns from amongst the immediately preceding (b-1) columns, with a linear combination of class-weight w or less of the columns from amongst any b consecutive columns.

In other words, a column h_j can be added provided that

$$h_j \neq (a_{i_1}h_{i_1} + \dots + a_{i_t}h_{i_t}) + (b_{g_1}h_{g_1} + \dots + b_{g_s}h_{g_s}), \qquad \dots \text{(eq 4.38)}$$

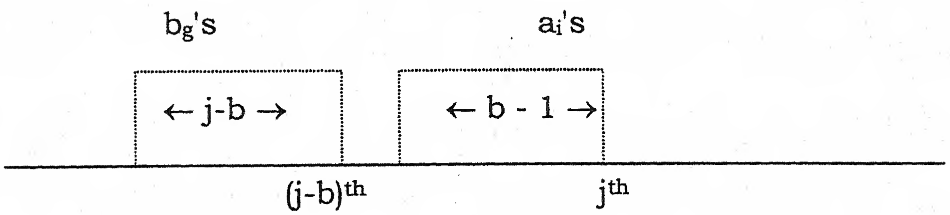
where $a_{i_1}h_{i_1} + \dots + a_{i_t}h_{i_t}$ is a linear combination of class-weight w-1 or less of columns from amongst the columns $h_{j-b+1}, h_{j-b+2}, \dots, h_{j-1}$ and $b_{g_1}h_{g_1} + \dots + b_{g_s}h_{g_s}$ is a linear combination of class-weight w or less of the columns from amongst any b consecutive columns out of $h_1, h_2, \dots, h_{j-1}$. This condition ensures that the syndromes of any two error patterns which are bursts of length b or less that are of class-weight w or less are always different.

The number of linear combinations of class-weight w or less of the columns from amongst any b consecutive columns out of h_1, h_2, ..., h_{j-1} can be obtained directly but some of the situations would repeat, we break up the analysis of these combinations into three different cases:

Case-I: When h_g's are taken from the first (j-b) columns, the number of ways in which the coefficient a_i can be selected is

$$V^{(b-1)}_{w-1,\mathcal{P}_1} \qquad \dots \text{(eq 4.39)}$$

The coefficients b_g's which form a



bursts of length b or less with class-weight w or less in a vector of length (j-b), can be selected (refer Theorem 4.10'), in

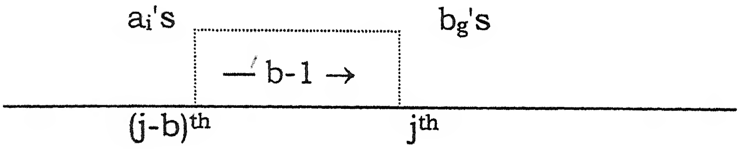
$$1+\sum_{i=1}^{b}\sum_{j=1}^{w}(j-b+1-i)\left\{A^{(i)}_{j,\mathcal{P}1}-2A^{(i-1)}_{j,\mathcal{P}1}+A^{(i-2)}_{j,\mathcal{P}1}\right\} \qquad \text{... (eq 4.40)}$$

ways.

Therefore, the total number of choice of coefficients in this case is

$$V^{(b-1)}_{w-1,\mathcal{P}1}\left[1+\sum_{i=1}^{b}\sum_{j=1}^{w}(j-b-i+1)\left\{A^{(i)}_{j,\mathcal{P}1}-2A^{(i-1)}_{j,\mathcal{P}1}+A^{(i-2)}_{j,\mathcal{P}1}\right\}\right] \qquad \text{... (eq 4.41)}$$

Case-II: When h_g's are taken from the immediately preceding

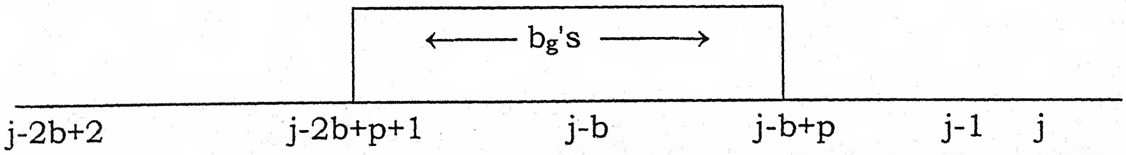


b-1 columns h_{j-b+1}, h_{j-b+2}, ..., h_{j-1}.

In this case, we have to select the coefficients a_i's and b_g's, with sum of their class-weights not exceeding 2w-1, from amongst (b-1) components viz. (j-b+1), ... , (j-1). Since coefficients having sum of their class-weights not exceeding w-1 have already been accounted in expression (eq 4.39), the additional number of ways to choose a_i's and b_g's is

$$V^{(b-1)}_{2w-1,\mathcal{P}1}-V^{(b-1)}_{w-1,\mathcal{P}1}=V^{(b-1)}_{2w-1,w-1,\mathcal{P}1} \qquad \text{... (eq 4.42)}$$

Case-III: When h_g's are selected from h_{j-2b+2}, h_{j-2b+3}, ..., h_{j-1} such that all are neither taken from $h_{j-2b+2},h_{j-2b+3},\ldots,h_{j-b}$ nor from $h_{j-b+1},h_{j-b+2},\ldots,h_{j-1}$.



In this case, let us assume that bursts starts from (j-2b+k+1)th component, which may obviously continue upto (j-b+k)th components. Let the nonzero coefficient in (j-2b+k+1)th component be of class-weight l with $1 \le l \le m-1$. Therefore, the number of choice in (j-2b+k+1)th component is

$$|B_l| \qquad \text{... (eq 4.43)}$$

Thus, we are to select nonzero entries b_g's with sum of their class-weights not exceeding $(w-l)$ in components from (j-2b+k+2)th to (j-b+k)th with the condition that the sum of class-weights of entries in components from (j-2b+k+2)th to (j-b)th does not exceed $(w-l-1)$, which is essential in view of the condition stated in the beginning of case III, that not all h_g's are to be selected from $h_{j-2b+2},\ldots,h_{j-b}$.

Also corresponding to the condition on h_i's, we are to select nonzero entries a_i's with sum of their class-weights not exceeding w-1 in components from (j-b+1)th to (j-1)th.

In order to do so, let us choose a set of nonzero entries, with sum of their class-weights equal to r_{1_l} in (j-2b+k+2)th to (j-b)th components; a set of nonzero entries with sum of their class-weights equal to r_{2_l} in $(j-b+1)$th to (j-b+k)th components and a set of nonzero entries with sum of their class-weight equal to r_{3_l} in (j-b+k+1)th to (j-1)th components, where

$$0 \le r_{1_l} \le w - l - 1 \qquad 1 \le r_{2_l} \le 2w - l - 1$$

$$\text{and} \quad 0 \le r_{3_l} \le w - 1, \qquad 1 \le l \le \min\{m-1, w-1\} \qquad \text{... (eq 4.44)}$$

Keeping in view the situation considered in Case-I and II, $r_{1_l}, r_{2_l}, r_{3_l}$ should further satisfy

$$r_{2_l} + r_{3_l} \geq w \text{ and} r_{1_l} + r_{2_l} + r_{3_l} \leq 2w - l - 1 \qquad \text{... (eq 4.45)}$$

Such a selection of coefficient including that for (j-2b+k+1) given us

$$\sum_{k=1}^{b-1} \sum_{l=1}^{m-1} r_{1_\ell}, \sum_{r_{1\ell}, r_{2\ell}, r_{3\ell}} \left|B_l\right| A^{(b-k-1)}_{r_{1_\ell}, \mathcal{P}_1} A^{(k)}_{r_{2_\ell}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_\ell}, \mathcal{P}_1} \qquad \text{... (eq 4.46)}$$

possible linear combinations, where r_{1_l}, r_{2_l} and r_{3_l} satisfy (eq 4.44) and (eq 4.45) and $A^{(n)}_{t,\mathcal{P}_1}$ is given by (eq 3.18) and (eq 3.20). Thus, from (eq 4.41), (eq 4.42) and (eq 4.46), the total number of choices of coefficients is

$$V^{(b-1)}_{w-1,\mathcal{P}_1}\left[1 + \sum_{i=1}^{b} \sum_{j=1}^{w} (j-b-i+1)\left\{A^{(i)}_{j,\mathcal{P}_1} - 2A^{(i-1)}_{j,\mathcal{P}_1} + A^{(i-2)}_{j,\mathcal{P}_1}\right\}\right] + V^{(b-1)}_{2w-1,w-1,\mathcal{P}_1}$$

$$+ \sum_{k=1}^{b-1} \sum_{l=1}^{m-1} \sum_{r_{1_l} r_{2_l} r_{3_l}} \left|B_l\right| A^{(b-k-1)}_{r_{1_l}, \mathcal{P}_1} A^{(k)}_{r_{2_l}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_l}, \mathcal{P}_1} \qquad \text{... (eq 4.47)}$$

where $r_{1_l}, r_{2_l}, r_{3_l}$ satisfy (eq 4.44) and (eq 4.45)

The jth column can be added if all the q^r r-tuples have not been exhausted by the conditional combinations.

In the worst case, all these might be distinct and therefore j^{th} column can always be added if

$$q^r > \text{(total number of combinations in eq 4.47)} \qquad \text{... (eq 4.48)}$$

But for an (n, k) linear code of given length n and having the desired error-correcting capability, to exist, relations (eq 4.48) should hold for j=n and r=n-k, so that it is possible to add upto n^{th} column to form an (n-k) × n matrix.

Corollary 4.9: If in the hypothesis of the above theorem we take w = (m-1)b, then the class-weight constraint consideration becomes superfluous, as no burst of length b or less can have class-weight more than (m-1)b. Therefore it is interesting, to examine what form the inequality (eq 4.37) takes.

For w = (m-1)b, we have

$$V^{(b-1)}_{w-1,\mathcal{P}_1} = V^{(b-1)}_{(m-1)b-1,\mathcal{P}_1} = V^{(b-1)}_{(m-1)(b-1),\mathcal{P}_1}$$

from (eq 3.21) as (m-1)(b-1) ≤ (m-1)b-1, (m≥2)

$$= \text{number of all (b-1)-tuples} = q^{b-1} \qquad \text{... (eq 4.49)}$$

and

$$\sum_{i=1}^{b} \sum_{j=1}^{(m-1)b} (n-b-i+1) \left\{ A^{(i)}_{j,\mathcal{P}_1} - 2A^{(i-1)}_{j,\mathcal{P}_1} + A^{(i-2)}_{j,\mathcal{P}_1} \right\}$$

= the number of bursts of lengths b or less having class-weight (m-1)b or less (excluding all-zero vectors) in the spaces of (n-b)-tuples (c.f. from Lemma 4.2')

= the number of bursts of length b or less in the space of (n-b) –tuples

$$= q^{b-1}[(n-2b+1)(q-1)+1]-1 \qquad \text{... (eq 4.50)}$$

(from the proof of Theorem 4.4)

Further

$$V^{(b-1)}_{2(m-1)b-1,\mathcal{P}_1} - V^{(b-1)}_{(m-1)b-1,\mathcal{P}_1} = V^{(b-1)}_{(m-1)(b-1),\mathcal{P}_1} - V^{(b-1)}_{(m-1)(b-1),\mathcal{P}_1} = 0$$

(from eq 3.21) ... (eq 4.51)

Also,

$$\sum_{k=1}^{b-1} \sum_{l=1}^{m-1} \sum_{r_{1_l}, r_{2_l}, r_{3_l}} |B_1| A^{(b-k-1)}_{r_{l_l},\mathcal{P}_1} A^{(k)}_{r_{2_l},\mathcal{P}_1} A^{(b-k-1)}_{r_{3_l},\mathcal{P}_1} = 0 \qquad \text{... (eq 4.52)}$$

follows from the fact that there does not exist any pair r_2, r_3 for which the requirement that $r_{2_l} + r_{3_l} \geq w(=(m-1)b)$ from last b-1 positions, on the summation is the fulfilled, as the maximum class-weight of entries in (b-1) positions does not exceed (m-1)(b-1).

Substituting (eq 4.49), (eq 4.50), (eq 4.51) and (eq 4.52) in (eq 4.37) we get

$$q^{n-k} > q^{2(b-1)}\left[(n-2b+1)(q-1)+1\right] \qquad \text{... (eq 4.53)}$$

Inequality (eq 4.53) is also a sufficient condition for the existence of an (n, k) linear code correcting all bursts of length b or less, given by Campopiano (c.f. Theorem 4.17, Peterson and Weldon, 1972).

In determining the bound (eq 4.37) in Theorem 4.11, we have tried to formulate the result for fixed values of n, k, w and b. It is always appropriate to maximize the length n of the code keeping its error - correcting capability and number of parity - check symbols intact. If this is taken as the basis of formulation of the problem, then we may alternatively state the result of Theorem 4.11 in the following form:

Theorem 4.12: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q that determines the class-metric under consideration in the space of n-tuples over Z_q, q prime and two positive integers w and b such that $2b \leq n$ and $w \leq (m-1)b$, it is always possible to construct an (n, k) linear code that corrects all bursts of length b or less that are of class-weight w or less is given by

$$q^{n-k} \leq V^{(b-1)}_{w-1,\mathcal{P}_1}\left[1+\sum_{i=1}^{b}\sum_{j=1}^{w}(n-b-i+2)\left\{A^{(i)}_{j,\mathcal{P}_1}-2A^{(i-1)}_{j,\mathcal{P}_1}+A^{(i-2)}_{j,\mathcal{P}_1}\right\}\right]+V^{(b-1)}_{2w-1,w-1,\mathcal{P}_1}$$

$$+\sum_{k=1}^{b-1}\sum_{l=1}^{m-1}\sum_{r_{1_l},r_{2_l},r_{3_l}}|B_l|\,A^{(b-k-1)}_{r_{1_l},\mathcal{P}_1}A^{(k)}_{r_{2_l},\mathcal{P}_1}A^{(b-k-1)}_{r_{3_l},\mathcal{P}_1} \quad \ldots \text{(eq 4.54)}$$

where

$$0 \leq r_{l_1} \leq w-l-1, \quad 1 \leq r_{2_l} \leq 2w-l-1, \quad 0 \leq r_{3_l} \leq w-1$$

$$r_{2_l}+r_{3_l} \geq w; \qquad r_{1_l}+r_{2_l}+r_{3_l} \leq 2w-l-1$$

and $1 \le l \le \min\{m-1, w-1\}$

$V^{(n)}_{t,\mathcal{P}_1}, A^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t_1,t_2,\mathcal{P}_1}$ are given by (eq 3.19), (eq 3.18) and (eq 3.26) respectively.

Proof: In the proof of Theorem 4.11, let n be the largest value of j for which inequality (eq 4.48) holds. Then for j = n+1 the inequality (eq 4.48) gets reversed. Therefore, there exists an (n, k) linear code with the desired error-correcting capabilities, which satisfies the inequality (eq 4.54).

The particular case of the result in the Theorem 4.12 for Hamming metric is taken up in the next corollary.

Corollary 4.10: Given positive integers w and b such that 2w ≤ 2b ≤ n, there exists an (n, k) linear code over Z_q, q prime that corrects all bursts of length b or less with (Hamming) weight w or less satisfying the inequality.

$$q^{n-k} \le \left\{\sum_{t=0}^{w-1}\binom{b-1}{t}(q-1)^t\right\}\left\{q^{w-1}\left[(q-1)(n-b-w+2)+1\right]\right.$$
$$\left.+(q-1)^2\sum_{i=w+1}^{b}(n-b-i+2)\sum_{t=0}^{w-2}\binom{i-2}{t}(q-1)^t\right\}$$
$$+\sum_{t=w}^{2w-1}\binom{b-1}{t}(q-1)^t+\sum_{k=1}^{b-1}\sum_{r_1,r_2,r_3}\binom{b-k+1}{r_1}\binom{k}{r_2}\binom{b-k-1}{r_3}(q-1)^{r_1+r_2+r_3+1}$$

... (eq 4.55)

where

$$0 \le r_1 \le w-2, \qquad 1 \le r_2 \le 2w-2, \qquad 0 \le r_3 \le w-1$$

$$r_2 + r_3 \ge w \qquad r_1 + r_2 + r_3 \le 2w-2$$

Proof: From (eq 3.22) and (eq 3.23) we have

$$A^{(p)}_{s,\mathcal{P}_H} = \binom{p}{s}(q-1)^s \qquad \text{... (eq 4.56)}$$

and $$V^{(p)}_{s,\mathcal{P}_H} = \sum_{t=0}^{s} \binom{p}{t}(q-1)^t \qquad \text{... (eq 4.57)}$$

Further, making use of the fact that a burst of length one can have Hamming weight only one, a burst of length two can have Hamming weight only two and a burst of length 3 or more has Hamming weight greater than or equal to 2, we have

$$1 + \sum_{i=1}^{b} \sum_{j=1}^{w} (n-b-i+2)\left\{A^{(i)}_{j,\mathcal{P}_H} - 2A^{(i-1)}_{j,\mathcal{P}_H} + A^{(i-2)}_{j,\mathcal{P}_H}\right\}$$

(c.f. expression in (eq 4.54).

$$= 1 + (n-b+1)\, A^{(1)}_{1,\mathcal{P}_H} + (n-b)\, A^{(2)}_{2,\mathcal{P}_H}$$

$$+ \sum_{i=3}^{b} \sum_{j=2}^{w} (n-b-i+2)\left\{A^{(i)}_{j,\mathcal{P}_H} - 2A^{(i-1)}_{j,\mathcal{P}_H} + A^{(i-2)}_{j,\mathcal{P}_H}\right\}$$

$$= 1 + (n-b+1)\,(q-1) + (n-b)\,(q-1)^2$$

$$+ \sum_{i=3}^{b} (n-b-i+2) \sum_{j=2}^{w} \left\{\left[\binom{i}{j} - 2\binom{i-1}{j} + \binom{i-2}{j}\right]\right\}(q-1)^j$$

(because $A^{(t)}_{s,\mathcal{P}_H} = \binom{t}{s}(q-1)^s$)

$$=1+(n-b+1)(q-1)+(n-b)(q-1)^2$$

$$+(q-1)^2\sum_{i=3}^{w}(n-b-i+2)\sum_{j=2}^{w}\binom{i-2}{j-2}(q-1)^{j-2}$$

$$+\sum_{i=w+1}^{b}(n-b-i+2)\sum_{j=2}^{w}\binom{i-2}{j-2}(q-1)^{j-2}$$

$$=1+(n-b+1)(q-1)+(n-b)(q-1)^2+(q-1)^2\sum_{i=3}^{w}(n-b-i+2)q^{i-2}$$

$$+\sum_{i=w+1}^{b}(n-b-i+2)\sum_{j=2}^{w}\binom{i-2}{j-2}(q-1)^{j-2}$$

(for $3 \le i \le w$, $\sum_{j=1}^{w}\binom{i-2}{j-2}(q-i)^{i-2}=\sum_{j=1}^{i}\binom{i-2}{j-2}(q-1)^{i-2}=q^{i-2}$)

$$=q^{w-1}\left[(q-1)(n-b-w+2)+1\right]+(q-1)^2\sum_{i=w+1}^{b}(n-b-i+2)\sum_{t=0}^{w-2}\binom{i-2}{t}(q-1)^t$$

... (eq 4.58)

$$\left|B_\ell\right|=\left|B_1\right|=(q-1)$$ ... (eq 4.59)

Using (eq 4.56), (eq 4.58) and (eq 4.59) in (eq 4.54) we get the inequality (eq 4.55).

CHAPTER V

CONSTRAINTS OVER BURST ERROR-CORRECTING CODES

5.1 Introduction

5.2 Codes Detecting/Correcting Random and Burst Errors

CHAPTER V

CONSTRAINTS OVER BURST ERROR-CORRECTING CODES

5.1 Introduction

We have described in Chapter III the correction of random errors with reference to the newly introduced metric viz. class-metric. Chapter IV was devoted to the problems relating to codes detecting/correcting low-class-weight burst errors. In other words, the codes studied so far are capable of detecting/correcting specifically either, random errors or special type of bursts e.g., low-class-weight bursts having lengths not exceeding a pre-assigned number.

Actually, it is the unsuitability of random error-correcting codes for many practical situations that led to studies of burst-error correcting codes (c.f. Abramson (1959), Forney (1971), Farrell and Hopkins (1982), Daniel (1985), Blaum, Farrell and Tilborg (1986, 1988), Abdel-Ghaffar, McElice and Tilborg (1988), Blaum (1990), Zhang and Wolf (1990). However in many situations, it is quite possible that along with a burst due to lightening or some other reason, some random errors are also introduced in a message because of normal noise factors. In such situations, even the use of burst-error-correcting codes may not solve efficiently the problem of receiving messages correctly, as a code correcting bursts of length b or less fails to correct even a small number of random errors, if these lie outside a burst of length b. It may appear that in such cases codes correcting bursts of suitably larger lengths, so that random errors also included in bursts, may be appropriate. But these codes will not prove elegant particularly in situations, where lengths of bursts and the number of random errors outside a burst are small and such random errors are separated from the burst by comparatively large number of positions. To correct such errors, codes formulated in terms of only bursts use more parity-checks than are sufficient in a code suitably formulated in terms of random and burst errors simultaneously.

Codes detecting/correcting random errors and bursts with or without weight constraints have earlier been studied for Hamming metric by Sharma and Dass (1977), and for Lee metric by Sharma and Goel (1977).

In Section 5.2, we derive upper bounds on sufficient number of parity checks required in codes detecting/correcting random errors and bursts with class-weight constraints, simultaneously and separately. First, more general results i.e. results concerning bounds for codes detecting/correcting random errors simultaneously with low-class-weight bursts (bursts having class-weight less than or equal to a pre-assigned number) are established. Then other results are derived as corollaries of the corresponding results already established.

5.2 Codes Detecting/Correcting Random and Burst Errors

In this section, we obtain upper bounds on the sufficient number of parity-check digits for the existence of codes that

i) have minimum class-weight at least W_1 and have no burst of length b or less which is of class-weight W_2 or less as a code word,

ii) have minimum weight at least W_1 and correct all bursts of length b or less that are of class-weight W_2 or less,

iii) correct all random errors of class-weight W_1 or less simultaneously with all bursts of length b or less that are of class-weight W or less

Theorem 5.1: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots\ldots, B_{m-1}\}$ of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q and positive integers W_1, W_2 and b such that $W_1 \leq W_2 \leq (m-1)b$; a sufficient condition that there exists an (n, k) linear code with minimum class-weight at least W_1 that has no non-zero burst of length b or less which is of class-weight W_2 or less as a code word is

$$q^{n-k} > V^{(n-1)}_{w_1-2.\mathcal{P}_1} + V^{(b-1)}_{w_2-1,w_1-2,\mathcal{P}_1} \qquad \text{... (eq 5.1)}$$

where $V^{(n)}_{t,\mathcal{P}_1}$ and $V^{(n)}_{t_1,t_2,\mathcal{P}_1}$ are given by (3.19) and (3.26)

Proof: As in the previous chapter, the sufficient condition would follow by examining the possibilities of constructing an (n-k) X n parity-check matrix for the desired code.

Select a nonzero (n-k)-tuple as the first column of the parity-check matrix. After having selected (j-1) columns, jth column h_j can be added in the parity-check matrix provided that it fulfills the two requirements laid down below.

As a first requirement, since the code has minimum class-weight at least W_1, the column h_j to be added should be such that it is not a linear combination of class-weight W_1-2 or less of the columns from amongst previously selected (j-1) columns.

Linear combinations (nonzero) of class-weight W_1-2 or less of columns from amongst (j-1) columns can be had in

$$V^{(j-1)}_{w_1-2,\mathcal{P}_1} - 1 \qquad \text{... (eq 5.2)}$$

ways.

Next, since the code does not have any burst of length b or less that has class-weight W_2 or less as a code word, therefore h_j should not be a linear combination of class-weight W_2-1 or less of columns from amongst immediately preceding (b-1) columns viz. (j-1)th,......,(j-b+1)th columns. As linear combinations of class-weight W_1-2 or less have already been accounted for in (eq 5.2), we need to compute only linear combinations of class-weight W_2 −1 or less but of class-weight W_1-1 or more of columns from amongst (b-1) columns.

Linear combinations of class-weight W_2-1 or less and of class-weight W_1-1 or more of columns from amongst (b-1) immediately preceding columns can be had in

$$V^{(b-1)}_{w_2-1,w_1-2,\mathcal{P}_1} \qquad \text{... (eq 5.3)}$$

At worst, all these linear combinations might be distinct. Therefore h_j can be added to the matrix if

$$q^{n-k} - 1 > V^{(j-1)}_{w_1-2,\mathcal{P}_1} - 1 + V^{(b-2)}_{w_2-1,w_1-2,\mathcal{P}_1} \qquad \text{... (eq 5.4)}$$

But for the existence of an (n, k) code, inequality (eq 5.4) should hold for j = n so that it is always possible to add upto n columns in the matrix. Therefore, an (n, k) linear code with desired properties exists satisfying (eq 5.1).

Corollary 5.1: In the case of Hamming metric, i.e., when m-1 = 1 and $\mathcal{P}_1 = \mathcal{P}_H$, we have

$$V^{(p)}_{s,\mathcal{P}_H} = \sum_{i=0}^{s} \binom{p}{i} (q-1)^i \qquad \text{... (eq 5.5)}$$

from (eq 3.23).

Substituting (eq 5.5) in (eq 5.1), Theorem 5.1 takes the form;

A sufficient condition for the existence of an (n, k) linear code with minimum Hamming weight at least W_1, $W_1 \geq 1$, that has no nonzero burst of lengths b or less, $(n \geq b)$, which is of Hamming weight W_2 or less $(b \geq W_2 \geq W_1)$, is

$$q^{n-k} > \sum_{i=0}^{w_1-2} \binom{n-1}{i} (q-1)^i + \sum_{j=w_1-1}^{w_2-1} \binom{b-1}{j} (q-1)^j \qquad \text{... (eq 5.6)}$$

This condition in the case of Hamming metric is already established by Dass (1974).

Corollary 5.2: Similarly, in the case of Lee metric and q an odd prime, we have

m-1 = (q-1)/2; $\mathcal{P}_1 = \mathcal{P}_L$ and

$$V^{(p)}_{t,\mathcal{P}_L} = 2^p p! \sum_{s_i} \frac{1}{s_0! s_1! \ldots s_{(q-1)/2}!} \frac{1}{2^{s_0}} \qquad \text{... (eq 5.7)}$$

where $s_0 + s_1 + \ldots\ldots s_{(q-1)/2} = p$

and $s_1 + 2s_2 + \ldots + \frac{(q-1)}{2} s_{(q-1)/2} \le t$

(from eq 3.25)

substituting (eq 5.7) in (eq 5.1), we get, that a sufficient condition for the existence of an (n, k) linear code with minimum Lee-weight at least W_1, ($W_1 \ge 1$), that has no nonzero burst of length b or less ($b \le n$) which is of Lee-weight W_2 or less, $\left(\frac{(q-1)}{2} b \ge w_2 \ge w_1\right)$, is

$$q^{n-k} > 2^{n-1}(n-1)! \sum_{s_i} \frac{1}{s_0! s_1! \ldots s_{(q-1)/2}!} \frac{1}{2^{s_0}}$$

$$-2^{(b-1)}(b-1)! \sum_{t_i} \frac{1}{t_0! t_1! \ldots t_{(q-1)/2}!} \frac{1}{2^{t_0}} \qquad \text{... (eq 5.8)}$$

where summation in the first expression on R.H.S. of (eq 5.8) runs over s_i's satisfying

$$s_0 + s_1 + \ldots + s(q-1)/2 = (n-1)$$

and $$s_1 + 2s_2 + \ldots + \frac{(q-1)}{2} s_{(q-1)/2} \le w_1 - 2$$

and summation in the second expression on R.H.S. of (eq 5.8) runs over t_i's satisfying

$$t_0 + t_1 + \ldots + t_{(q-1)/2} = b - 1$$

and $$w_1 - 1 \le t_1 + 2t_2 + \ldots + \frac{q-1}{2} t_{(q-1)/2} \le w_2 - 1$$

Corollary 5.3: The result obtained in Theorem 5.1 has been proved for $W_1 \le W_2$. However if $W_1 > W_2$, then the burst criterion becomes redundant and

$$V^{(b-1)}_{w_2-1, w_1-2, \mathcal{P}_1} = 0 \qquad \text{from (eq 3.26)}$$

Then the condition (eq 5.1) in the theorem reduces to

$$q^{n-k} > V^{(n-1)}_{w_1-2, \mathcal{P}_1}$$

which is Varshamov-Gilbert-Sacks-Type bound for a linear code having minimum class-weight at least W$_1$ (c.f. Theorem 4.7, Peterson and Weldon, 1972).

Corollary 5.4: If we relax the class-weight constraint imposed over the code, i.e., if we set W$_1$ = 1, then

$$V^{(n-1)}_{w_1-2,\mathcal{P}_1} = V^{(n-1)}_{-1,\mathcal{P}_1} = 0 \qquad \text{... (eq 5.9)}$$

from (3.20).

Then the inequality in (eq 5.1) reduces to

$$q^{n-k} > V^{(b-1)}_{w_2-1,\mathcal{P}_1},$$

This coincides with the result obtained in Theorem 4.8 for the existence of an (n, k) code having no burst of lengths b or less which is of class-weight W$_2$ or less as a code word.

Corollary 5.5: Relaxing the class-weight constraint imposed over bursts, i.e., setting W$_2$ = (m-1)b, then

$$V^{(b-1)}_{w_2-1,w_1-2,\mathcal{P}_1} = V^{(b-1)}_{(m-1)b-1,w_1-2,\mathcal{P}_1} = V^{(b-1)}_{(m-1)((b-1),w_1-2,\mathcal{P}_1}$$

$$= q^{(b-1)} - V^{(b-1)}_{w_1-2,\mathcal{P}_1} \qquad \text{... (eq 5.10)}$$

Using (eq 5.10 in (eq 5.1) we get

$$q^{n-k} > V^{(n-1)}_{w_1-2,\mathcal{P}_1} + q^{b-1} - V^{(b-1)}_{w_1-2,\mathcal{P}_1} \qquad \text{... (eq 5.11)}$$

Hence (eq 5.11) gives a sufficient condition for the existence of an (n, k) linear code with minimum class-weight at least W_1 and having no burst of length b or less as a code word.

Corollary 5.6: Relaxing the class-weight constraints imposed over the code as well as over bursts, i.e., setting $W_1 = 1$ and $W_2 = (m-1)b$, by using (eq 5.9) and (eq 5.10) in (eq 5.1), the inequality in (eq 5.1) reduces to

$$q^{n-k} > q^{b-1}.$$

This coincides with the result obtained in Corollary 4.5 for the existence of a code having no burst of lengths b or less as a code word.

Next, we come to codes capable of detecting random errors upto a given class-weight and correcting burst errors with class-weight constraints.

For the proof of the main result, we need of the following lemma:

Lemma 5.1: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots\ldots, B_{m-1}\}$ of Z_q, determining the class-metric under consideration in the space of (j-b)-tuples over Z_q, q prime, the number of bursts of length b or less with class-weight $P_2 \geq 1$, is

$$(j-b)\left|B_{p_2}\right| + \sum_{f=2}^{\min\{b,j-b\}} (j-b-f+1) \sum_{\substack{2\leq l+l'\leq p_2 \\ l,l'\geq 1}} \left|B_l\right|\left|B_{l'}\right| A^{(f-2)}_{p_2-l-l',\mathcal{P}_1} \qquad \text{... (eq 5.12)}$$

where $\left|B_s\right|$ is the number of elements of Z_q having class-weight s and $A^{(n)}_{t,\mathcal{P}_1}$ is given by (eq 3.18).

Proof: Number of bursts of length 1 having class-weight P_2 is easily seen to be

$$(j-b)\left|B_{P_2}\right| \qquad \text{... (eq 5.13)}$$

Also, any burst of length f, $2 \le f \le \min\{b, j-b\}$, has

$$(j-b-f+1) \qquad \text{... (eq 5.14)}$$

starting positions in the space of (j-b)-tuples.

A burst of length f with class weight P_2 and starting from say r^{th} position has nonzero elements of class-weights l and l',(l, $l' \ge 1$; $2 \le l+l' \le P_2$) in r^{th} and $(r+f-1)^{th}$ positions. Number of choices for r^{th} and $(r + f - 1)^{th}$ positions is

$$\sum_{\substack{2\le l+l'\le P_2 \\ l,l'\ge 1}} \left|B_l\right|\left|B_{l'}\right| \qquad \text{... (eq 5.15)}$$

The remaining (f-2) positions viz. $(r+1)^{th}$,......,$(r+f-2)^{th}$ of the burst should have class-weight equal to p_2-l-l', (so that the class-weight of the burst of length f is P_2), number of choices for which is

$$A^{(f-2)}_{p_2 - l - l', \mathcal{P}_1} \qquad \text{... (eq 5.16)}$$

Thus denoting an expression by its number, the total number of the required bursts is equal to

$$\text{(eq 5.13)} + \sum_{f=2}^{b} \text{(eq 5.14) (eq 5.15)(eq 5.16)}$$

Now we come to the main result in which we obtain an upper bound on the number of check digits sufficient for the existence of an (n, k) linear code having minimum class-weight at least W_1 which is simultaneously capable of correcting all bursts of length b or less that are of class-weight W_2 or less.

This result generalizes Varshamov-Gilbert-Sacks bound and results due to Campopiano (1962), Sharma and Dass (1977). Also, it is an extension of Theorem 4.11.

Theorem 5.2: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0, B_1, \ldots\ldots, B_{m-1}\}$ of Z_q, q prime, that determines the class-metric under consideration in the space of n-tuples over Z_q; and positive integers W_1, W_2 and b such that $W_1 \leq 2W_2 \leq 2(m-1)b$, and $n < 2b$, a sufficient condition that there exists an (n, k) linear code with minimum class-weight at least W_1 that corrects all bursts of length b or less that are of class-weight W_2 or less, is

$$
\begin{aligned}
q^{n-k} > V^{(n-1)}_{w_1-2.\mathcal{P}_1} &+ \sum_{\substack{p_1,P_2 \\ p_1+p_2=w_1-1}}^{p_1+p_2=2w_2-1} A^{(b-1)}_{\mathcal{P}_1,\mathcal{P}_1}\Bigg\{(n-b)\left|B_{\mathcal{P}_2}\right| \\
&+ \sum_{f=2}^{b}(n-b+1-f)\sum_{\substack{2\le l+l'\le p_2 \\ l,l'\ge 1}}\left|B_l\right|\left|B_{l'}\right|A^{(f-2)}_{P_2-l-l',\mathcal{P}_1}\Bigg\} \qquad \dots \text{(eq 5.17)} \\
&+ V^{(b-1)}_{2w_2-1,d-1,\mathcal{P}_1} \\
&+ \sum_{k=1}^{b-1}\sum_{l_1=1}^{\min\{m-1,w_2-1\}}\sum_{r_{1_{l_1}},r_{2_{l_1}},r_{3_{l_1}}}\left|B_{l_1}\right|A^{(b-k-1)}_{r_{1_{l_1}},\mathcal{P}_1}A^{(k)}_{r_{2_{l_1}},\mathcal{P}_1}A^{(b-k-1)}_{r_{3_{l_1}},\mathcal{P}_l}
\end{aligned}
$$

where

$$0 \le P_1 \le W_2 - 1,\ 0 \le P_2 \le W_2,$$

$$d = \max.\ \{W_1 - 1, W_2\}$$

and

$$0 \le r_{1_{l_1}} \le w_2 - l_1 - 1,\ 1 \le r_{2_{l_1}} \le 2w_2 - l_1 - 1;\ 0 \le r_{3_{l_1}} \le w_2 - 1,$$

$$r_{2_{l_1}} + r_{3_{l_1}} \ge w_2,\quad w_1 - 2 \le r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \le 2w_2 - l_1 - 1,$$

$$1 \le l_1 \le \min\{m - 1, w_2 - 1\}$$

and

$V^{(n)}_{t,\mathcal{P}_1}$, $V^{(n)}_{t_1,t_2,\mathcal{P}_1}$ and $A^{(n)}_{t,\mathcal{P}_1}$ are given by (eq 3.19), (eq 3.26) and (eq 3.18) respectively.

Proof: As before, choose a nonzero (n-k)-tuple as the first column of the (n-k)xn parity-check matrix H. Subsequent columns to H should be added in such a way that after having selected j-1 columns $h_1,h_2,\dots\dots,h_{j-1}$ suitably, a nonzero (n-k)-tuple can be added as jth column to H, if it fulfills the two requirements laid down below.

As a first requirement, since the code is to have minimum class-weight at least W_1, the column h_j to be added should be such that it is not a linear combination of class-weight W_1-2 or less of the columns from amongst the previous columns. That is,

$$h_j \neq \left(a_{i_1} h_{i_1} + a_{i_2} h_{i_2} + \dots + a_{i_s} h_{i_s} \right) \qquad \text{... (eq 5.18)}$$

Where R.H.S. of inequality (eq 5.18) is a nonzero linear combination of class-weight W_1-2 or less of the columns from amongst the previous columns. The number of ways in which such linear combinations, (nonzero) can be had, is given by

$$V^{(j-1)}_{w_1-2,\mathcal{P}_1} - 1 \qquad \text{... (eq 5.19)}$$

Next, since the code is required to correct all error patterns which are bursts of length b or less that are of class-weight W_2 or less, we must ensure that h_j is not a sum of a linear combination of class-weight W_2-1 or less of the columns from amongst preceding b-1 columns and of a linear combination of class-weight W_2 or less of the columns from amongst any b consecutive columns taken out of previous j-1 columns.

In other words, h_j can be added provided that in addition to (eq 5.18), we have

$$h_j \neq \left(b_{g_1} h_{g_1} + \ldots + b_{g_t} h_{g_t}\right) + \left(c_{k_1} h_{k_1} + \ldots + c_{k_u} h_{k_u}\right) \qquad \ldots \text{(eq 5.20)}$$

Where $b_{g_1} h_{g_1} + \ldots + b_{g_t} h_{g_t}$ is a linear combination of class-weight W_2-1 or less of columns from amongst $h_{j-b+1,} \ldots, h_{j-1}$ and also $c_{k_1} h_{k_1} + \ldots + c_{k_n} h_{k_n}$ is a linear combination of class-weight W_2 or less of columns from amongst any b consecutive columns out of the previous j-1 columns.

Since all possible linear combinations of class-weight W_1-2 or less are already accounted for in (eq 5.19), the coefficients b_g's and c_k's should be so chosen that the sum of their class-weights is at least W_1-1. To obtain the number of all possible distinct linear combinations, we analyse the following three different cases:

Case I: When the h_k's are taken from the first j-b columns

In this case we choose b_g's having sum of their class-weights equal to the number P_1 and c_k's having sum of their class-weights equal to P_2 such that $P_1 + P_2 \geq W_1$-1. The largest values, which P_1 and P_2 can have, are W_2-1 and W_2 respectively.

Therefore,

$$W_1 - 1 \leq P_1 + P_2 \leq 2W_2 - 1$$

Now b_g's with sum of their class weights equal to P_1 can be chosen in

$$A^{(b-1)}_{p_1, \mathcal{P}_1} \qquad \text{... (eq 5.21)}$$

ways.

To choose c_k's with sum of their class-weights equal to P_2 is equivalent to evaluating the number of bursts of length b or less with class-weights P_2 in a vector of length (j-b). The required number, given by the Lemma 5.1, is

$$(j-b)\left|B_{p_2}\right| + \sum_{f=2}^{\min\{b, j-b\}} (j-b-f+1) \sum_{\substack{2 \leq l + l' \geq p_2 \\ l, l' \geq 1}} \left|B_l\right| \left|B_{l'}\right| A^{(f-2)}_{p_2 - l - l', \mathcal{P}_1} \qquad \text{... (eq 5.22)}$$

ways.

Case II: When the h_k are taken from the immediately preceding (b-1) columns.

In this case, we have to select the coefficients b_g's and c_k's, which have sum of their class-weights $2W_2$-1 or less from amongst b-1 components. Keeping in view the possibilities considered already, the additional number of ways in which these can be selected are

$$V^{(b-1)}_{2w_2 - 1, d-1, \mathcal{P}_1} \qquad \text{... (eq 5.23)}$$

where d = max [w_1-1,w_2].

Case III: When h_k's are selected from $h_{j-2b+2}, h_{j-2b+3},\ldots., h_{j-1}$ such that all are neither taken from $h_{j-2b+2}, h_{j-2b+3},\ldots, h_{j-b}$ nor from $h_{j-b+1}, h_{j-b+2},\ldots, h_{j-1}$.

In this case, let us suppose that the burst starts from (j-2b+k+1)th component and continues obviously to (j-b+k)th component. Also let the nonzero entry in (j-2b+k+1)th position has class-weight l_1. Then number of choices for (j-2b+k+1)th component is obviously

$$\left|B_{l_1}\right| \qquad \text{... (eq 5.24)}$$

Our object is to select nonzero components from j-2b+k+2, j-2b+k+3,.........,j-b+kth positions having sum of their class weights W_2-l_1 or less together with nonzero components from j-b+1,j-b+2,......,j-1th positions, having sum of their class-weights W_2-1 or less.

In order to do so, let us choose nonzero components from j-2b+k+2,j-2b+k+3,......,j-bth positions having sum of their class-weights $r_{1_{l_1}}$ or less; from j-b+1, j-b+2,......, j-b+kth positions having sum of their class-weights $r_{2_{l_1}}$ or less, and from j-b+k+1, j-b+k+2, ..., j-1th positions having sum of their class-weight $r_{3_{l_1}}$ or less, where

$$1 \le l_1 \le \min\{m-1, w_2 - 1\}, 0 \le r_{1_{l_1}} \le w_2 - l_1 - 1,\ 1 \le r_{2_{l_1}} \le 2w_2 - 1_1 - 1,$$

$$0 \le r_{3_{l_1}} \le w_2 - 1 \qquad \text{(eq 5.25)}$$

Keeping in view situations considered in Case I and Case II earlier $r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}$ should further satisfy

$$r_{2_{l_1}} + r_{3_{l_1}} \ge w_2, w_1 - 2 \le r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \le 2w_2 - l_1 - 1 \qquad \text{... (eq 5.26)}$$

Such a selection of coefficients from (j-2b+k+1)th position and from (j-2b+k+2), (j-2b+k+3),......, (j-1)th positions gives us

$$\sum_{k=1}^{b=1} \sum_{l_1=1}^{m-1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_{l_1}\right| A^{(b-k-1)}_{r_{1_{l_1}}, \mathcal{P}_1} A^{(k)}_{r_{2_{l_1}}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}}, \mathcal{P}_1} \qquad \text{... (eq 5.27)}$$

Where $r_{1_{l_1}}, r_{2_{l_1}}$ and $r_{3_{l_1}}$ satisfy the constraints given by (eq 5.25) and (eq 5.26).

Thus, from (eq 5.19), (eq 5.21), (eq 5.22), (eq 5.23), (eq 5.27), the total number of choices of coefficients is

$$(6.19) + \sum_{\substack{p_1, p_2 \\ p_1 + p_2 = w_1 - 1}}^{p_1 + p_2 = 2w_2 - 1} (6.21)(6.22) + (6.23) + (6.27) \qquad \text{... (eq 5.28)}$$

Where an expression is denoted by its number.

If the number $q^{n-k}-1$ of all nonzero (n-k)-tuples is greater than this, then certainly a vector h_j can be added as jth column ($j \leq n$) for all choices of the coefficients, i.e., h_j can be added provided that

$$q^{n-k}-1 > \text{(total number of combinations in (eq 5.28)} \qquad \text{... (eq 5.29)}$$

But for an (n, k) linear code to exist, inequality (eq 5.29) should hold for $j = n$, so that it is always possible to add nth column to the matrix.

Therefore, an (n, k) linear code with desired properties always exits satisfying (eq 5.17).

Remarks: For Hamming metric, the result corresponding to that of Theorem 5.2 has been obtained by Sharma and Dass (1977). It can be obtained by making the following substitutions in the statement of Theorem 5.2:

$m-1 = 1$, $\mathcal{P}_1 = \mathcal{P}_H = \{B_0, B_1\}$, $B_1 = \{1,2,\ldots,(q-1)\}$

$$A^{(p)}_{t,\mathcal{P}_1} = A^{(p)}_{t,\mathcal{P}_H} = \binom{p}{t}(q-1)^t$$

$$V^{(p)}_{t,\mathcal{P}_1} = V^{(p)}_{t,\mathcal{P}_H} = \sum_{i=1}^{t}\binom{p}{i}(q-1)^i$$

$$|B_l| = |B_1| = q-1.$$

Also, the result for Lee metric and q an odd prime, corresponding to that of Theorem 5.2 can be obtained by making the following substitutions in the statement of Theorem 5.2:

$$m - 1 = (q - 1)/2,\ \mathcal{P}_1 = \mathcal{P}_L = \{B_0, B_1, \ldots, B_{(q-1)/2}\},\ B_i = \{i, q - i\}$$

and

$$A^{(p)}_{t,\mathcal{P}_1} = A^{(p)}_{t,\mathcal{P}_L} = 2^p p! \sum_{s_i} \frac{1}{s_0! s_1! .. s_{(q-1)/2}!} \frac{1}{2^{s_0}}$$

where $s_0 + s_1 + \ldots + s_{(q-1)/2} = p$

and $s_1 + 2s_2 + \ldots + \frac{(q-1)}{2} s_{(q-1)/2} = t$

and $V^{(p)}_{t,\mathcal{P}_1} = V^{(p)}_{t,\mathcal{P}_L} = \sum_{i=1}^{t} A^{(p)}_{i,\mathcal{P}_L}$

and $|B_l| = 2.$

Corollary 5.7: The result of Theorem 5.2 has been proved for $W_1 \leq 2W_2$. If we take $W_1 > 2W_2$, the minimum class-weight of the code becomes at least $2W_2+1$, then the code is capable of correcting errors of class-weight W_2 or less and hence, in particular, all burst of length b or less that are of class-weight W_2 or less. Thus the burst criterion becomes redundant and the bound in (eq 5.17), because of the conclusions of (i), (ii) and (iii) below reduces to the Varshamov-Gilbert-Sacks-Type bound viz.

$$q^{n-k} > V^{(n-1)}_{w_1-2,\mathcal{P}_1}$$

as obtained in Section 3.4.

The bound has been obtained from (eq 5.17) by making of the following three conclusions based on $W_1 > 2W_2$ viz.

i) the condition $w_1 - 1 \le p_1 + p_2 \le 2w_2 - 1$ cannot be satisfied along with $w_1 > 2w_2$ by any pair of positive integers P_1 and P_2 and hence

$$\sum_{\substack{p_1, p_2 \\ p_1+p_2=w_1-1}}^{p_1+p_2=2w_2-1} A^{(b-1)}_{p_1,\mathcal{P}_1} \left\{ (n-b)\left|B_{p_2}\right| + \sum_{f=2}^{b} (n-b-f+1) \sum_{\substack{2<l+l'\le p_2 \\ l,l'\ge 1}} \left|B_l\right| \left|B_{l'}\right| A^{(f-2)}_{p_2-l-l',\mathcal{P}_1} \right\} = 0$$

(ii) $d = \max\{w_1 - 1, w_2\} = w_1 - 1$

therefore

$V^{(b-1)}_{2w_2-1,d-1,\mathcal{P}_1} = V^{(b-1)}_{2w_2-1,w_1-2,\mathcal{P}_1}$ = number of (b-1)-tuples having class-weight more than W_1-2 and less than or equal to $2W_2$-1 = 0

and

iii) the condition

$$w_1 - 2 \le r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \le 2w_2 - l_1 - 1, l_1 \ge 1$$

cannot be satisfied by any triplet $\left(r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}\right)$ in view of the inequality W$_1$ > 2W$_2$ and therefore

$$\sum_{k=1}^{b-1} \sum_{l_1=1}^{m-1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_{l_1}\right| A^{(b-k-1)}_{r_{1_{l_1}}, \mathcal{P}_1} A^{(k)}_{r_{2_{l_1}}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}}, \mathcal{P}_1} = 0$$

Corollary 5.8: Relaxing the weight constraint imposed over the code i.e., putting W$_1$ = 1; P$_1$ + P$_2$ would take values from 0 to 2W$_2$-1. Then condition $0 \le P_1 + P_2 \le 2w_2-1$ along with $0 \le P_1 \le w_2-1$, $0 \le p_2 \le w_2$ implies that the joint summation involving P$_1$, P$_2$ on two factors in (eq 5.17) would split into two separate summations giving

$$\sum_{p_1=0}^{w_2-1} A^{(b-1)}_{p_1, \mathcal{P}_1} = V^{(b-1)}_{w_2-1, \mathcal{P}_1}$$

and

$$\sum_{p_2=0}^{w_2} \left\{ (n-b)\left|B_{p_2}\right| + \sum_{f=2}^{b} (n-b-f+1) \sum_{\substack{2 \le l+l' \le p_2 \\ l, l' \ge 1}} \left|B_l\right| \left|B_{l'}\right| A^{(f-2)}_{p_2-l-l', \mathcal{P}_1} \right\}$$

= number of bursts of length b or less that are of class weight W$_2$ or less including the pattern of all zero in the space of (n-b)-tuples

$$= 1 + \sum_{i=1}^{b} \sum_{j=1}^{w_2} (n-b-i+1) \left\{ A^{(i)}_{j, \mathcal{P}_1} - 2A^{(i-1)}_{j, \mathcal{P}_1} + A^{(i-2)}_{j, \mathcal{P}_1} \right\}$$

(c.f. Lemma 4.2' and Theorem 4.1')

Also, as

$$d = \max\{w_1 - 1, w_2\} = w_2$$

$$V^{(b-1)}_{2w_2-1, d-1, \mathcal{P}_1} = V^{(b-1)}_{2w_2-1, w_2, \mathcal{P}_1} = V^{(b-1)}_{2w_2-1, \mathcal{P}_1} - V^{(b-1)}_{2w_2-1, \mathcal{P}_1}$$

The bound in (eq 5.17) thus reduces to the result obtained in Theorem 4.11 for an (n, k) linear code that corrects all bursts of length b or less that are of class-weights W_2 or less.

Next, relaxing the class-weight constraints imposed over burst to be corrected, i.e. setting $W_2 = (m-1)b$, so that expression in (eq 5.17) is valid among other conditions, for

$$r_{2_{l_1}} + r_{3_{l_1}} \geq w_2 = (m-1)b \qquad \text{... (eq 5.30)}$$

But, since the number of components out of which $r_2 + r_3$ can be chosen is (b-1), therefore

$$r_{2_{l_1}} + r_{3_{l_1}} \not> (m-1)(b-1) \qquad \text{... (eq 5.31)}$$

In view of (eq 5.30) and (eq 5.31), there cannot exist any r_2 and r_3 and hence

$$\sum_{k=1}^{b-1} \sum_{l_1=1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_{l_1}\right| A^{(b-k-1)}_{r_{1_{l_1}}, \mathcal{P}_1} A^{(k)}_{r_{2_{l_1}}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}}, \mathcal{P}_1}$$

Also

$$d = \max\lfloor w_1 - 1, (m-1)b \rfloor$$

Therefore d-1 ≥ (m-1)b-1.

As no (b-1)-tuple, can have class-weight more than (m-1)(b-1) and hence more than d-1, therefore

$$V^{(b-1)}_{2w_2-1,d-1,\mathcal{P}_1} = 0$$

Thus, in case there is no class-weight constraint over bursts, Theorem 5.2, in view of the preceding discussion reduce to

Corollary 5.9: Given a $\mathcal{P}$-partition $\mathcal{P}_1 = \{B_0,B_1,\ldots,B_{m-1}\}$, of Z_q, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q and two positive integers w and b such that $W \leq 2(m-1)b$ and $2b < n$, a sufficient condition that there exists an (n, k) linear code having minimum class-weight at least w that corrects all bursts of length b or less, is

$$q^{n-k} > V^{(n-1)}_{w-2,\mathcal{P}_1} + \sum_{\substack{p_1,p_2 \\ p_1+p_2=w-1}}^{2(m-1)b-1} A^{(b-1)}_{p_1,\mathcal{P}_1}\left\{(n-b)\left|B_{p_2}\right|\right.$$

$$\left. + \sum_{f=2}^{b}(n-b-f+1)\sum_{\substack{2\leq l+l'\leq p_2 \\ l,l'\geq 1}}\left|B_l\right|\left|B_{l'}\right|A^{(f-2)}_{p_2-l-l',\mathcal{P}_1}\right\}$$

The above corollary in the case of Hamming metric reduces to a result due to Sharma and Dass (1977).

Corollary 5.10: Relaxing the class-weight constraints imposed over the code as well as over the bursts i.e. setting $W_1 = 1$ and $W_2 = (m-1)b$, then from the considerations as given in Corollary 4.9 and in Corollary 5.8 and Corollary 5.9, the result obtained in Theorem 5.2 reduces to sufficient condition for the existence of an (n, k) linear code that corrects bursts of length b or less to

$$q^{n-k} > q^{2(b-1)}\left[(q-1)(n-2b+1)+1\right]$$

Which has been already reduced as Corollary 4.9 in this thesis and was given originally by Campopiano (c.f. Theorem 4.17, Peterson and Weldon, 1972).

We have stated in Chapter II that the random class-error correcting capability of a code depends on its minimum class-weight. More precisely, a code with minimum class-weight w or less is capable of correcting all errors patterns of class-weight $\left\lfloor \frac{w-1}{2} \right\rfloor$ or less. But this is true when the code is to correct random errors only. However, if the code is to correct burst errors also in addition to random errors, then a code with minimum class-weight at least w may fail to correct all random errors of class-weight $\left\lfloor \frac{w-1}{2} \right\rfloor$ or less. The reason for the failure is that the syndrome corresponding to a burst error may be the same as the syndrome corresponding to a random error-pattern of class-weight $\left\lfloor \frac{w-1}{2} \right\rfloor$ or less.

For similar reasons the codes considered in Theorem 5.2, which detect all error patterns of class-weight W_1-1 or less that correct all bursts of length b or less which have class-weight W_2 or less may not serve to correct all random errors of class-weight $\left\lfloor \frac{w_1-1}{2} \right\rfloor$ or less simultaneously with all bursts of length b or less that are of class-weight W_2 or less. Therefore, the codes correcting later type of error-patterns have to be considered separately. In the next theorem we obtain upper bounds on the sufficient number of parity-check digits for the existence of such a code.

For the main result we need the following

Lemma 5.2: Given a $\mathcal{P}$-partition, $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$, of Z_q q prime, determining the class-metric in the space of (j-1)-tuples over Z_q, the number of bursts of length b or less with class-weight $P_1 \geq 1$ is

$$(j-1)\left|B_{P_1}\right| + \sum_{f=2}^{\min\{b,i-j\}} (j-f) \sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \left|B_l\right|\left|B_{l'}\right| A^{(f-2)}_{p_1-l-l',\mathcal{P}}$$

where $A^{(n)}_{t,\mathcal{P}_1}$ is given by (3.18).

Proof: Number of bursts of length 1 having class-weight P_1 is seen to be

$$(j-1)\left|B_{p_1}\right| \qquad \text{... (eq 5.32)}$$

Also, any burst of length $f \geq 2$, $f \leq \min\{b, j-1\}$, has

$$(j-f) \qquad \text{... (eq 5.33)}$$

starting positions. A burst of length f with class-weight equal to P_1 and starting from say rth position has non-zero elements of class-weights say l and l', ($l \geq 1$, $l' \geq 1$, $2 \leq l+l' \leq p_1$) in rthand (r+f-1)th positions. Number of choices for rth and (r+f-1)th Position together is

$$\sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \left|B_l\right|\left|B_{l'}\right| \qquad \text{... (eq 5.34)}$$

The entries in the remaining (f-2) positions viz. (r+1)th, (r+2)th,……,(r+f-2)th of the burst should have sum of their class-weights equal to P_1-l-l' (so that the class-weight of the burst of length f is p_1), the number of choices for such entries is

$$A^{(f-2)}_{p_1, l-l', \mathcal{P}_1} \qquad \text{... (eq 5.35)}$$

Thus, denoting an expression by its number, the total number of desired bursts is equal to

$$(6.32) + \sum_{f=2}^{\min\{b, j-1\}} (6.33)(6.34)(6.35)$$

Now we come to the proof of the main result.

Theorem 5.3: Given a $\mathcal{P}$-partition $\mathcal{P}_1=\{B_0,B_1,\ldots,B_{m-1}\}$ of $\mathbb{Z}_q$, q prime, determining the class-metric under consideration in the space of n-tuples over Z_q, and positive integers W_1, W_2 and b such that $W_1 < W_2 \leq (m-1)b$, $2b < n$, a sufficient condition that there exists an (n, k) linear code that corrects all combinations of class-weights W_1 or less and bursts of length b or less that are of class-weight W_2 or less, is

$$q^{n-k} > V^{(n-1)}_{2w_1-1,\mathcal{P}_1} + \sum_{\substack{p_1,p_2\\ p_1+p_2=2w_1}}^{p_1+p_2=w_1+w_2-1} A^{(n-1)}_{p_2,\mathcal{P}_1}\Bigg\{(n-1)\left|B_{p_1}\right|$$

$$\left. + \sum_{f=2}^{n-1}(n-f)\sum_{\substack{2\leq l+l'\leq p_1\\ l,l'\geq 1}}\left|B_l\right|\left|B_{l'}\right|A^{(f-2)}_{P_1-l-l',\mathcal{P}_1}\right\}$$

$$+ V^{(b-1)}_{w_2-1,w_1-1,\mathcal{P}_1}A^{(n-b-1)}_{w_1,P_1} + \Bigg\{(n-b)\sum_{p_1=w_1+1}^{w_2}\left|B_{p_1}\right|$$

$$\left. + \sum_{f=2}^{n-1}(n-b-f+1)\sum_{\substack{2\leq l+l'\leq p_1\\ l,l'\geq 1}}\left|B_l\right|\left|B_{l'}\right|\sum_{p_1=w_1+1}^{w_2}A^{(f-2)}_{p_1-l-l'_{l},l',\mathcal{P}_1}\right\} \qquad \text{(eq 5.36)}$$

$$+ V^{(b-1)}_{2w_2-1,w_1+w_2-1,\mathcal{P}_1} + \sum_{k=1}^{b-1}\sum_{l_1=1}^{m-1}\sum_{r_{1_{l_1}},r_{2_{l_1}},r_{3_{l_1}}}\left|B_{l_1}\right|A^{(b-k-1)}_{r_{1_{l_1}},\mathcal{P}_1}A^{(k)}_{r_{2_{l_1}},\mathcal{P}_1}A^{(b-k-1)}_{r_{3_{l_1}},\mathcal{P}_1}$$

where $0 \leq P_1 \leq w_2$, $0 \leq P_2 \leq w_1 - 1$

$$0 \leq r_{1_{l_1}} \leq w_2 - l_1 - 1,\ 1 \leq r_{2_{l_1}} \leq 2w_2 - l_1 - 1,\ 0 \leq r_{3_{l_1}} \leq w_2 - 1$$

$$r_{2_{l_1}} + r_{3_{l_1}} \ge w_2,\ w_1 + w_2 - 1 \le r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \le 2w_2 - l_1 - 1$$

$$1 \le l_1 \le \min\{m - 1, w_2 - 1\}$$

Proof: As before, the sufficient condition would follow by examining the possibilities of constructing an (n-k) x n parity-check matrix H for the desired code.

Select a nonzero (n-k)-tuple as the first column of the parity-check matrix. After having selected j-1 columns, jth column h_j can be added in the parity-check matrix if it fulfills three requirements laid down below.

As a first requirement, since the code is to correct all error-patterns of class-weight W_1 or less, the column h_j to be added should be such that it is not a linear combination (nonzero) of class-weight $2W_1$-1 or less of the columns from amongst the previous j-1 columns, which can be chosen in

$$V^{(j-1)}_{2w_1-1,\mathcal{P}_1} - 1 \qquad \text{... (eq 5.37)}$$

ways.

Next, since the code is to correct all bursts of length b or less that are of class-weight W_2 or less along with all error-patterns of class-weight W_1 or less, therefore the syndrome of any burst of length b or less which is of class-weight W_2 or less should not be equal to that of any error of class-weight W_1 or less.

Inequality (eq 5.38) below assures that the syndrome of any error pattern of class-weight W$_1$ or less is not equal to that of any error pattern which is a burst of length b or less having class-weight W$_2$ or less out of j components except in the particular case when the burst pattern includes the last component (i.e. jth component) and at the same time the random error-pattern of exactly class-weight W$_1$ having been selected from the first j-b-1 components, which is now taken care of by the inequality (eq 5.39).

Therefore, the second requirement on h$_j$ is that

$$h_j \neq \left(a_{i_1}h_{i_1} + a_{i_2}h_{i_2} + \dots + a_{i_\alpha}h_{i_\alpha}\right) + \left(b_{k_1}h_{k_1} + \dots + b_{k_\beta}h_{k_\beta}\right) \qquad \dots \text{(eq 5.38)}$$

and

$$h_j \neq \left(c_{s_1}h_{s_1} + \dots + c_{s_r}h_{s_r}\right) + \left(d_{t_1}h_{t_1} + \dots + d_{t_\beta}h_{t_\beta}\right) \qquad \dots \text{(eq 5.39)}$$

where $a_{i_1}h_{i_1} + .,.. + a_{i_\alpha}h_{i_\alpha}$ is any linear combination of class-weight W$_2$ or less (> 2) of the columns from amongst a set of b consecutive columns; $b_{k_1}h_{k_1} + b_{k_2}h_{k_2} + \dots + b_{k_\beta}h_{k_\beta}$ is a linear combination of class-weight W$_1$-1 or less of columns from amongst h_1, h_2, h_{j-1}; $c_{s_1}h_{s_1} + \dots + c_{s_r}h_{s_r}$ is a linear combination of class-weight W$_2$-1 or less of the columns from amongst $h_{j-b+1}, h_{j-b+2}, \dots, h_{j-1}$ and $d_{t_1}h_{t_1} + \dots + d_{t_\beta}h_{t_\beta}$ is a linear combination of class-weight W$_1$ of the columns from amongst h$_1$,h$_2$,....,h$_{j-b-1}$.

Since all possible linear combinations of class-weight $2W_1$-1 or less of every combinations of columns are included in (eq 5.37), therefore we should choose coefficients in (eq 5.38) and (eq 5.39) such that

$$w_2 + w_1 - 1 \ge \sum w_{\mathcal{P}_1}(a_i) + \sum w_{\mathcal{P}_1}(b_k) \ge 2w_1$$

and

$$w_2 - 1 \ge \sum w_{\mathcal{P}_1}(c_s) \ge w_1 \qquad \text{... (eq 5.40)}$$

In order to do so let

$$\sum w_{\mathcal{P}_1}(a_i) = p_1 \qquad \text{and} \qquad \sum w_{\mathcal{P}_1}(b_k) = p_2$$

such that

$$w_2 + w_1 - 1 \ge p_1 + p_2 \ge 2w_1 \qquad \text{... (eq 5.41)}$$

The largest values which P_1 and P_2 can attain are W_2 and W_1-1 respectively.

Now a_1's, which form a burst of length b or less having class-weight P_1 in a vector of length j-1, can be selected, by the Lemma 5.2, in

$$(j - 1)\left|B_{P_1}\right| + \sum_{f=2}^{\min\{b.j-1\}} (j - f) \sum_{\substack{2 \le l + l' \le p_1 \\ l,l' \ge 1}} \left|B_l\right|\left|B_{l'}\right| A^{(f-2)}_{p_1 - l - l', \mathcal{P}_1} \qquad \text{... (eq 5.42)}$$

ways.

And b_k's having sum of their class-weights equal to P_2 in (j-1)-tuple space can be selected in

$$A^{(j-1)}_{p_2, \mathcal{P}_1} \qquad \text{... (eq 5.43)}$$

way

Further c_s's can be chosen in

$$V^{(b-1)}_{w_2-1, w_1-1, \mathcal{P}_1} \qquad \text{... (eq 5.44)}$$

ways, whereas the number of ways in which d_t's can be selected is

$$A^{(j-b-1)}_{w_1., \mathcal{P}_1} \qquad \text{... (eq 5.45)}$$

From (eq 5.42), (eq 5.43), (eq 5.44) and (eq 5.45), the total number of choices of coefficients meeting the second requirement is

$$\sum_{\substack{p_1, p_2 \\ p_1+p_2=2w_1}}^{p_1+p_2=w_2+w_1-1} A^{(j-1)}_{p_2,\mathcal{P}_1}\left\{(j-1)\left|B_{p_1}\right|\right.$$

$$+\sum_{f=2}^{\min\{j-1,b\}}(j-f)\sum_{\substack{2\le l+l'\le p_1 \\ l,l'\ge 1}}\left|B_l\right|\left|B_{l'}\right|A^{(f-2)}_{p_1-l-l'}$$

$$+V^{(b-1)}_{w_2-1,w_1-1,\mathcal{P}_1}\;A^{(j-b-1)}_{w_1,\mathcal{P}_1} \qquad \text{... (eq 5.46)}$$

The third and last requirement on h_j is to be determined keeping in view that syndromes of any two bursts of length b or less that are of class-weight W_2 or less must be distinct. Therefore, the third requirement is that

$$h_j \neq \left(e_{u_1}h_{u_1}+\ldots+e_u h_u\right)+\left(f_{v_1}h_{v_1}+\ldots+f_{v_\theta}h_{v_\theta}\right) \qquad \text{... (eq 5.47)}$$

Where $e_{u_1}h_{u_1}+\ldots+e_u h_u$ is any linear combination of class-weight W_2-1 or less of the columns from amongst $h_{j-b+1}, h_{j-b+2},\ldots, h_{j-1}$ and $f_{v_1}h_{v_1}+\ldots+f_{v_\theta}h_{v_\theta}$ is any linear combination of class-weight W_2 or less of columns from a set of b consecutive columns out of all previous j-1 columns. We analyse this situation in three different cases.

Case I: When h_v's are taken from the first j-b columns. In this case, keeping in view the situations considered earlier, e_u's and f_v's should be such that

$$\sum w_{\mathcal{P}_1}(e_u) \ge w_1 \text{ and } w_2 \ge \sum w_{\mathcal{P}_1}(f_v) \ge w_1 + 1 \qquad \text{... (eq 5.48)}$$

The number of e_u's satisfying (eq 5.48) is given by (eq 5.44) whereas f_v's which form a burst of length b or less with class-weight W_1+1 or more but of class-weight W_2 or less in a vector of length (j-b) can be chosen (refer Lemma 5.2) in

$$(j-b)\sum_{p_1=w_1+1}^{w_2}\left|B_{p_1}\right|$$
$$+\sum_{f=2}^{\min\{b,j-b\}}(j-b-f+1)\sum_{\substack{2\le l+l'\le p_1\\ l,l'\ge 1}}\left|B_l\right|\left|B_{l'}\right|\sum_{p_1=w_1+1}^{w_2}A^{(f-2)}_{p_1-l-l',\mathcal{P}_1}$$

... (eq 5.49)

ways.

Thus, number of choices of the coefficients in Case I is

$$V^{(b-1)}_{w_2-1,w_1-1,\mathcal{P}_1}\Bigg[(j-b)\sum_{p_1=w_1+1}^{w_2}\left|B_{p_1}\right| \qquad \text{... (eq 5.50)}$$
$$+\sum_{f=2}^{\min\{b,j-b\}}(j-b-f+1)\sum_{\substack{2\le l+l'\le p_1\\ l,l'\ge 1}}\left|B_l\right|\left|B_{l'}\right|\sum_{p_1=w_1+1}^{w_2}A^{(f-2)}_{p_1-l-l',\mathcal{P}_1}$$

Case II: When hh_v's are taken from the immediately preceding b-1 columns $h_{j-b+1}, h_{j-b+2}, \ldots, h_{j-1}$.

In this case, we have to select the coefficients e_u's and f_v's, having sum of their class-weights $2W_2$-1 or less from amongst b-1 components. Keeping in view the possibilities considered uptil now, the additional number of ways in which these can be selected are

$$V^{(b-1)}_{2w_2-1, w_1+w_2, \mathcal{P}_1} \qquad \text{... (eq 5.51)}$$

Case III: When h_v's are taken from $h_{j-2b+2}, h_{j-2b+3}, \ldots, h_{j-1}$ such that all are neither taken from $h_{j-2b+2}, h_{j-2b+3}, \ldots, h_{j-b}$ nor from $h_{j-b+1}, h_{j-b+2}, \ldots, h_{j-1}$.

Considering the same situations as in Theorem 5.2, it suffices to evaluate the ranges of $r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}$, which may be taken as follows:

$$0 \le r_{1_{l_1}} \le w_2 - l_1 - 1,\ l \le r_{2_{l_1}} \le 2w_2 - l_1 - 1,\ 0 \le r_{3_{l_1}} \le w_2 - 1,$$

$$r_{2_{l_1}} + r_{3_{l_1}} \ge w_2,\ w_1 + w_2 - 1 \le r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \le 2w_2 - l_1 - 1$$

$$1 < l_1 \le \min\{m-1, w_2 - 1\} \qquad \text{... (eq 5.52)}$$

Thus, the number of coefficients in this case is

$$\sum_{k=1}^{b-1} \sum_{l_1=1}^{m-1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_{l_1}\right| A^{(b-k-1)}_{r_{1_{l_1}}, \mathcal{P}_1} A^{(k)}_{r_{2_{l_1}}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}}, \mathcal{P}_1} \qquad \text{... (eq 5.53)}$$

Where $l_1, r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}$ satisfy (eq 5.52). Thus from (eq 5.37), (eq 5.46), (eq 5.50), (eq 5.51) and (eq 5.53) total number of (nonzero) linear combinations is

$$V^{(j-1)}_{2w_2-1, \mathcal{P}_1} - 1 + \sum_{\substack{p_1, p_2 \\ p_1+p_2=2w_1}}^{p_1+p_2=w_1+w_2-1} A^{(j-1)}_{p_2, \mathcal{P}_1} \left\{ (j-1) \left|B_{p_1}\right| \right.$$

$$+ \sum_{f=2}^{\min\{b, j-1\}} (j-f) \sum_{\substack{2 \le l+l' \le p_1 \\ l, l' \ge 1}} \left\{ \left|B_l\right| \left|B_{l'}\right| A^{(f-2)}_{p_1-l-l', \mathcal{P}_1} \right\}$$

$$+ V^{(b-1)}_{w_2-1, w_1-1, \mathcal{P}_1} \left[A^{(j-b-1)}_{w_1, \mathcal{P}_1} + \left\{ (j-b) \sum_{p_1=w_1+1}^{w_2} \left|B_{p_1}\right| \right. \right.$$

$$+ \sum_{f=2}^{\min\{j-1, b\}} (j-b-f+1) \sum_{\substack{2 \le l+l' \le P_1 \\ l, l' \ge 1}} \left|B_l\right| \left|B_{l'}\right| \sum_{p_1=w_1+1}^{w_2} A^{(f-2)}_{p_1-l-l', \mathcal{P}_1}$$

$$+ V^{(b-1)}_{2w_2-1, w_1+w_2-1, P_1} + \sum_{k=1}^{b-1} \sum_{l_1=1}^{m-1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_l\right| A^{(b-k-1)}_{r_{1_{l_1}}, \mathcal{P}_1} A^{(k)}_{r_{2_{l_1}}, \mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}}, \mathcal{P}_1}$$

... (eq 5.54)

for j ≤ n, column h_j can be added in the matrix provided that

$q^{n-k} - 1 >$ total number of combinations in (eq 5.54) ... (eq 5.55)

But for the existence of an (n, k) code, inequality (eq 5.55) should hold for j = n so that it is always possible to add nth column to the matrix. Therefore an (n, k) linear code with desired properties always exists satisfying (eq 5.36).

Remarks: A result for Hamming metric correspond to that of the above theorem (c.f. Sharma and Dass, 1977) giving an upper bound on the sufficient number of parity-check symbols for an (n, k) linear code that corrects all combinations of W_1 or fewer errors and all bursts of length b or less that are of Hamming weight W_2 or less can be obtained by making the following substitutions in the statement of Theorem 5.3:

$$P_1 = \mathcal{P}_H = \{B_0, B_1\} \qquad B_1 = \{1, 2, \ldots, q-1\}; \ m - 1 = 1$$

$$A^{(s)}_{t,\mathcal{P}_H} = \binom{s}{t}(q-1)^t, \ V^{(s)}_{t,\mathcal{P}_H} = \sum_{i=0}^{t}\binom{s}{i}(q-1)^i$$

$$V^{(s)}_{t_1,t_2,\mathcal{P}_H} = \begin{cases} V^{(s)}_{t_1,\mathcal{P}_H} - V^{(s)}_{t_2,\mathcal{P}_H} & \text{if } t_1 \geq t_2 \\ 0 & \text{if } t_1 \leq t_2 \end{cases}$$

and

$$\left|B_t\right| = \begin{cases} 1 & \text{if } t = 0 \\ q - 1 & \text{if } t = 1 \\ 0 & \text{if } t > 1 \end{cases}$$

Similarly, a result corresponding that of Theorem 5.3 for Lee metric may be obtained by making the following substitutions in Theorem 5.3:

$$\mathcal{P}_1 = \mathcal{P}_L = \left\{B_0, B_1, \ldots., B_{(q-1)/2}\right\} \text{ for (q an odd prime)}$$

where $B_i = \{i, q\text{-}i\}$. $i = 1,2,\ldots\ldots\ldots,(q\text{-}1)/2$

$m\text{-}1 = (q\text{-}1)/2$

$$A^{(s)}_{t,\mathcal{P}_L} = 2^s s! \sum_{s_i} \frac{1}{s_0! s_1! \ldots s_{(q-1)/2}!} \frac{1}{2^{s_0}}$$

where summation runs over s_i satisfying

$$s_0 + s_1 + \ldots\ldots\ldots + s_{(q-1)/2} = s$$

and $$s_1 + 2s_2 + \ldots. + \frac{(q-1)}{2} s_{(q-1)/2} = t$$

$$V^{(s)}_{t,\mathcal{P}_L} = \sum_{i=0}^{s} A^{(s)}_{t,\mathcal{P}_L}$$

and

$$B_t = \begin{cases} 1 & \text{if } t = 0 \\ 2 & \text{if } (q-1)/2 \geq t \geq 1 \\ 0 & \text{if } t > (q-1)/2 \end{cases}$$

Corollary 5.11: The result obtained in the preceding theorem has been proved for W₁ < W₂. However if we take W₁ ≥ W₂ then the code is capable of correcting all random errors of class-weight W₁ or less and in particular all bursts of length b or less that are of class-weight W₂ or less. Therefore the burst consideration becomes redundant. Also then many expressions in (eq 5.54) become zero as shown below

$$\sum_{\substack{p_1, p_2 \\ p_1+p_2=2w_1}}^{p_1+p_2=w_1+w_2-1} A^{(j-1)}_{p_2,\mathcal{P}_1} \Big\{ (j-1) \Big| B_{p_1} \Big|$$

$$+ \sum_{f=2}^{\min\{b,j-1\}} (j-f) \sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \Big|B_l\Big| \Big|B_{l'}\Big| \sum_{p_1=w+1}^{w_2} A^{(f-2)}_{p_1-l-l',\mathcal{P}_1} \Big\}$$

$$= \sum_{p_1+p_2=2w_2}^{p_1+p_2 \leq 2w_2} A^{(j-1)}_{p_2,\mathcal{P}_1} \Big\{ (j-1) \Big\{ \Big| B_{p_1} \Big|$$

$$+ \sum_{f=2}^{\min\{b,j-1\}} (j-f) \sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \Big|B_l\Big| \Big|B_{l'}\Big| \sum_{p_1=w_1+1}^{w_2} A^{(f-2)}_{p_1-l-l',\mathcal{P}_1} \Big\} = 0$$

As summation sums from P₁ + P₂ = 2W₂ to P₁ + P₂ ≤ 2W₂

$$V^{(b-1)}_{w_2-1,w_1-1,\mathcal{P}_1} = 0 \quad \text{as} \quad w_2 \leq w_1$$

Similarly

$$V^{(b-1)}_{2w_2-1,w_1+w_2-1,\mathcal{P}_1} = 0 \quad \text{as} \quad 2w_2 - 1 \leq w_1 + w_2 - 1$$

and

$$\sum_{k=1}^{b-1} \sum_{l_1=1}^{m-1} \sum_{r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}} \left|B_{l_1}\right| \left|B_{l'}\right| A^{(b-k-1)}_{r_{1_{l_1}},\mathcal{P}_1} A^{(k)}_{r_{2_{l_1}},\mathcal{P}_1} A^{(b-k-1)}_{r_{3_{l_1}},\mathcal{P}_1} = 0$$

as $w_1 + w_2 - 1 \leq r_{1_{l_1}} + r_{2_{l_1}} + r_{3_{l_1}} \leq 2w_2 - l_1 - 1$ cannot be satisfied by any set of $r_{1_{l_1}}, r_{2_{l_1}}, r_{3_{l_1}}$ when $w_2 \leq w_1$ and $l_1 \geq 1$.

Therefore expression (eq 5.54) reduces to

$$V^{(j-1)}_{2w_1-1,\mathcal{P}_1} - 1$$

so that the bound takes the form

$$q^{n-k} > V^{(n-1)}_{2w_1-1,\mathcal{P}_1}$$

The result thus reduces to Varshamov-Gilbert-Sacks-Type bound obtained in Chapter IV, for a code correcting all error patterns of class-weight W1 or less.

Corollary 5.12: Relaxing the error-correction constraint i.e., putting $W_1 = 0$, the joint summation on two factors involving P_1 and P_2 in the inequality (eq 5.36) vanishes since this splits into product of two separate summations and one of them viz.

$$\sum_{p_2=0}^{w_1-1} A^{(n-1)}_{p_2,\mathcal{P}_1}$$

vanishes for $W_1 = 0$.

Further, for $W_1 = 0$, we have

$$V^{(b-1)}_{w_2-1,w_1-1,\mathcal{P}_1} = V^{(b-1)}_{w_2-1,-1,\mathcal{P}_1} = V^{(b-1)}_{w_2-1,\mathcal{P}_1}$$

Also as

$$A^{(n-b-1)}_{w_1,\mathcal{P}_1} + \left\{(n-b)\sum_{p_1=w_1+1}^{w_2} \left|B_{p_1}\right|\right.$$

$$\left. + \sum_{f=2}^{b}(n-b-f+1) \sum_{\substack{2\le l+l'\le p_1 \\ l,l'\ge 1}} \left|B_l\right|\left|B_{l'}\right| \sum_{p_1=w_1+1}^{w_2} A^{(f-2)}_{p_1-l-l',\mathcal{P}_1}\right\} \qquad \text{... (eq 5.56)}$$

denotes the number of bursts of lengths b or less having class-weights (W_1+1) or more and W_2 or less in an (n-b)-tuple space.

Therefore for W₁ = 0, (eq 5.56) reduces to the number of bursts of lengths b or less that are of class-weight W₂ or less in the space of (n-b)-tuples is given by

$$1+\sum_{i=1}^{b}\sum_{j=1}^{w}(n-b-i+1)\left\{A^{(i)}_{j,\mathcal{P}_1}-2A^{(i-1)}_{j,P_1}+A^{(i-2)}_{j,\mathcal{P}_1}\right\}$$

(Using Lemma 4.2')

and

$$V^{(b-1)}_{2w_2-1,w_1-1,\mathcal{P}_1}=V^{(b-1)}_{2w_2-1,w_2-1,\mathcal{P}_1}=V^{(b-1)}_{2w_2-1,\mathcal{P}_1}-V^{(b-1)}_{w_2-1,\mathcal{P}_1}$$

Thus inequality (eq 5.36) reduces to the sufficient condition obtained in Theorem 4.11 for the existence of an (n, k) linear code that corrects all bursts of length b or less that are of class-weight W₂ or less.

Again, if we relax the class-weight constraint imposed over the bursts to be corrected i.e., putting W₂ = (m-1)b the expression (eq 5.53) vanishes because

$$r_{2_{l_1}}+r_{3_{l_1}}\geq(m-1)b \qquad \text{(by eq 5.52)}$$

Where $r_{2_{l_1}}$ and $r_{3_{l_1}}$ are to be the sum of class-weights of entries in b-1 places. This is impossible because out of b-1 positions, the maximum class-weight of the entries does not exceed (b-1)(m-1). Also for

$$w_2 = (m-1)b; \qquad V^{(b-1)}_{2(m-1)b-1,\, w_1+(m-1)b-1,\, \mathcal{P}_1} = 0$$

as in (b-1)-tuple space there is no vector of class-weight W_1 + (m-1)b, or more ($W_1 \geq 1$).

Hence the theorem reduces to

Corollary 5.13: Given a $\mathcal{P}$-Partition $\mathcal{P}_1 = \{B_0, B_1, \ldots, B_{m-1}\}$ of Z_q, q prime, that determines the class-metric under consideration in the space of n-tuples over Z_q, and two positive integers W_1 and b such that $W_1 < (m-1)b$, $2b < n$, a sufficient condition that there exists an (n, k) linear code that corrects all combinations of class-weight W_1 or less and all bursts of length b or less, is

$$q^{n-k} > V^{(n-1)}_{2w_1-1,\mathcal{P}_1} + \sum_{\substack{p_1, p_2 \\ p_1+p_2=2w_1}}^{p_1+p_2=(m-1)b+w_1-1} A^{(n-1)}_{p_2,\mathcal{P}_1} \Bigg\{ (n-1) \left| B_{p_1} \right|$$

$$+ \sum_{f=2}^{n-1} (n-f) \sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \left| B_l \right| \left| B_{l'} \right| A^{(f-2)}_{p_1-l-l',\mathcal{P}_1} \Bigg\}$$

$$+ V^{(b-1)}_{(m-1)b-1,\, w_1-1,\, \mathcal{P}_1} \Bigg[A^{(n-b-1)}_{w_1,\mathcal{P}_1} + \Bigg\{ (n-b) \sum_{p_1=w_1+1}^{(m-1)b} \left| B_{p_1} \right|$$

$$+ \sum_{f=2}^{b} (n-b-f+1) \sum_{\substack{2 \leq l+l' \leq p_1 \\ l,l' \geq 1}} \left| B_l \right| \left| B_{l'} \right| \sum_{p_1=w_1+1}^{(m+1)b} A^{(f-2)}_{p_1-l-l',\mathcal{P}_1} \Bigg\} \Bigg]$$

where $0 \le P_1 \le (m-1)b$ and $0 \le P_2 \le W_1-1$

and

$$A^{(n)}_{t,\mathcal{P}_1} \text{ and } V^{(n)}_{t,\mathcal{P}_1} \text{ and } V^{(n)}_{t_1,t_2,\mathcal{P}_1}$$

Are given by (eq 3.18), (eq 3.19) and (eq 3.20).

Corollary 5.14: Relaxing the random error correction constraint as well as the class-weight constraint imposed over the bursts, i.e., putting $W_1 = 0$ and $W_2 = (m-1)b$, the bound obtained in the theorem reduces to sufficient condition for the existence of an (n, k) linear code that corrects all bursts of lengths b or less (refer corollary 4.8) reducing the expression (eq 5.36) to

$$q^{n-k} > q^{2(b-1)}\left[(q-1)(n-2b+1)+1\right]$$

which is a result due to Campopiano (c.f. Theorem 4.17, Peterson and Weldon, 1972).

Concluding Remarks

Ever increasing amount of data carrying multimedia information, from all walks of life including from the field of entertainment and education, is being transmitted, received and processed.

Almost whole of the digital data is expressed in terms of only binary codes. However, in view of the fact that binary alphabet is very small, the length of the messages have to be very large. The significant advantage achievable by increasing the size of the alphabet, can be easily guessed from the fact that even if the alphabet size is increased just from 2 to 3, the number of words representable with 8 ternary letters is more than 25 times of the number of words representable with 8 binary letters (3^8 = 6,561 ternary words as against 2^8 = 256 binary words). Even if the length of a message is a few thousand letters - gain in using ternary alphabet is astronomical. And, if the size of the alphabet is taken still larger, the gain in terms of the number of letters required to represent messages is much more.

In this work, we have suggested a method using which larger sizes of alphabets can be profitably used, because of the fact that for each practical channel using larger alphabet sets, we can find an appropriate metric using the method.

Once the method suggested in the thesis, for generating suitable metrics for channels using larger alphabet, is in place, there is need for deriving suitable encoding and decoding schemes for messages over larger alphabet sets. In this respect we have derived some basic results. However, there is enough scope for the work based on what has been incorporated in the thesis.

References

1. Abdelabaki, H; Gelenbe, E and El-Khyamy, S E, "Random Neural Network Decoder for Error Correcting Codes," *IJCNN'99, International Joint Conference on Neural Networks*, IEEE, Piscataway, NJ, Vol. 5, pp. 3241-3245, July 1999.

2. Abdel-Ghaffar, K A S, McEliece, R J and Tilborg, H C A, "Two Dimensional Bursts Identification Codes and Their Use in Burst Correction," *IEEE, Transactions on Information Theory*, Vol. 34, no 3, p. 494-504, May 1988.

3. Abramson, N M, "A Class of Systematic Codes for Non-Independent Errors," *IRE, Transaction on Information*, Vol. 5, p. 150-157, 1959.

4. Adamek, *Foundation of Coding Theory and Application of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*, John Wiley US, 1991.

5. Ahlswede, R, Bassalygo, L A and Pinsker, M S, "On the Hamming Bound for Nonbinary Localized Error-Correcting Codes," *Problems of Information Transmission*, Vol. 2, pp. 117-124, April-June 1999.

6. Al-Bassam, S and Bose B, "On Balanced Code", *IEEE, Transactions on Information Theory*, Vol. 36, No. 2, pp. 406-408, 1990.

7. Anderson, J B, *Digital Transmission Engineering*, IEEE Press US, New York, 1999.

8. Arikan, E, "An Implementation of Elias Coding of Input Restricted Channels," *IEEE Transactions on Information Theory*, Vol. 36, No. 1, pp.160-162, 1990.

9. Arikan, E, "On the Achievable Rate Region of Sequential Decoding Error Class of Multi-Access Channels," *IEEE Transactions on Information Theory*, Vol. 36, pp. 180-183, 1990.

10. Berger T; "Feaviobonomi Capacity and Zero-Error Capacity of Issuing channels," *IEEE Transactions on Information Theory*, Vol. 36 No. 1, pp. 173-179, September 1988.

11. Berlekamp, E R, "Negacyclic Codes for the Lee Metric in R C Bose and T A Dowling (eds)," *Combinatorial Mathematics*, University of North Carolina Press, pp.298-316, 1969.

12. Berlekamp, E R, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

13. Berreu, C and Glavieux, A, "Near Optimum Error-Correcting Codes and Decoding," *IEEE, Transactions Communication*, Vol. 44, pp. 1261-1271, October 1996.

14. Blahut, R, *Principles and Practice of Information Theory*, Addison-Weseley, 1987.

15. Blahut, R, *Theory and Practice of Error Control Codes*, Addison-Weseley, 1983.

16. Blaum, M, "A Family of Efficient Burst-Correcting Array codes," *IEEE Transactions on Information Theory,* Vol. 36, No. 3, pp. 671-675, May 1990.

17. Blaum, M, Farrell, P G and Tilborg, H C A, "A Class of Burst Error Correcting Array Codes," *IEEE, Transactions on Information Theory*, Vol. 32, no. 6, p. 836-839, November, 1986.

18. Blaum, M, Farrell, P G and Tilborg, H C A, "Multiple Burst Correcting Error Codes," *IEEE, Transactions on Information Theory*, Vol. 34, no. 5, p. 1061-1066, September, 1988.

19. Boley J P and Gils, W J V, "Cater for Combined Symbol and Digital Error Control," *IEEE Transactions on Information Theory*, Vol.34, No.5, p.1286-1307, September 1988.

20. Bose R C and Chaudhuri, D K R, "Further Results on Error Correcting Binary Group Codes," *Information and Control*, Vol. 3, pp. 279-290, 1960.

21. Brue, J and Blaum, M, "Neural Networks, Error Correcting Codes and Polynomials over the Binary N-cube," *IEEE Transactions on Information Theory*, Vol. 34, No. 5, pp. 976-987, September 1988.

22. Buchmann, J and Hohalt, T (eds), "Coding Theory, Cryptography and Related Areas," Proceedings of an International Conference on Coding Theory, Cryptography and Related Areas held in Guanajuata, Mexico, Berlin-Springer-Verlag, De, April 1998.

23. Calderbank, A R and Sloane, N J A, "An Eight Dimensional Trellis Code," Proceedings of IEEE, Vol. 74, p. 757-759, 1986.

24. Campopiano, C N, "Bounds on Burst Error Correcting codes," *IEEE, Transactions on Information Theory*, Vol. 8, p. 257-259, 1962.

25. Canway J H and Sloane, N J A, "Lexicographic Codes: Error Correcting Codes From Game Theory," *IEEE Transactions on Information Theory*, Vol 32, no. 3, , p. 337-348, May 1986.

26. Cesizer, I and Narain, P, "Arbitrarily Varying Channels with Constrained Inputs and States," *IEEE, Transactions on Information Theory*, Vol. 34, no 1, p. 27-35, January 1988.

27. Cesizer, I and Narain, P, "Capacity and Decoding Rules for Classes of Arbitrarily Varying Channels," *IEEE, Transactions on Information Theory*, Vol. 35, no. 4, p. 752-769, July 1989.

28. Cesizer, I and Narain, P, "The Capacity of Arbitrarily Varying Channel Revisited: Positivity, Constraints," *IEEE, Transactions on Information Theory*, Vol. 34, no. 2, p. 181-193, March 1988.

29. Chan, W C, Geraniotis, E and Nguyen, V D, "An Adaptive Hybrid FEC/ARQ Protocol Using Turbo Codes," *IEEE 6th International Conference on Universal Person Communications Record, Bridging the way to the 21st Century, ICUPC*, Vol. 2, pp. 541-545, 1997.

30. Chattopadhyay S and Chaudhari, P P, "Parallel Decoder for Cellular Automata Based Byte Error Correcting Codes," Proceedings of Tenth International Conference on VLSI Design, *IEEE* Computer Society Press, pp. 527-528, 1997.

31. Chen, C L, "Error Correcting Codes for Byte Organized Memory Systems," *IEEE Transactions on Information Theory*, Vol 32 no. 2, p. 181-185, March 1986.

32. Chen, C L, "Linear Codes for Masking Memory Defects," *IEEE Transactions on Information Theory*, vol. 31, no. 1, p. 105-106, Jan. 1985.

33. Chen, W and Honkalo, H S, "Lower Bounds for q-Ary Covering Codes," *IEEE, Transactions on Information Theory*, Vol. 36, no 3, p. 664-671, May 1990.

34. Cheng, J, and Watanabe, Y, "A Multiuser k-Ary Code for Noisy Multiple Access Adder Channel," *IEEE, Transactions on Information Theory*, Vol. 47, no 6, p. 2603-2607, September 2001.

35. Chiang, C Y and Wolf, J K, "On Channels and Codes for Lee Metric," *Information and Control*, Vol. 19, p. 159-173, 1971.

36. Chiu, M C, "DC-Free Error-Correcting Codes based on Convolutuional Codes," *IEEE Transactions on Communications*, Vol. 49, no.4 p.609-19, USA, April 2001.

37. Clark, W E and Liang, J J, "Equidistant Binary Arithmetic Codes," *IEEE Transactions on Information Theory*, vol 32, no. 1, p. 106-108, Jan. 1986.

38. Cleju L and Sirbu, A, "A new class of Error Correcting Codes," *IEEE International Symposium on Information Theory, IEEE*, New York, pp. 266, 1998.

39. Conway J H and Sloane, N J A, "Quaternary Constructions for the Binary Single Error Correcting Codes of Julin, Best, and others," *Designs, Codes and Cryptography*, Vol. 41, pp. 31-42, 1994.

40. D'yachkov, A G, Macula, A J Jr. and Rykov, V V, "New Constructions of Superimposed Codes," *IEEE Transactions on Information Theory*, Vol. 46, No. 1, pp. 284-290, January 2000.

41. Daniel, J S, "Double Burst Error Correcting codes, Generation and Decoding," Presented at IEEE International Symposium on Information Theory, Brighton, UK, June 1985.

42. Das, A K and Chaudhari, P P, "Ancient Characterization of Cellular Automata," Proceeding IEE (part E), Vol. 137, pp. 81-87, January 1990.

43. Dass, B K, "On Error Correction Capabilities of Burst Code with Weight Constraints, PhD Thesis 1974.

44. DeJonghe, A and Vandendorpe, L," An Overview of Some Turbo Techniques in Digital Communication," *Revue HF*, No. 1, p.38-50, Belgium, 2001.

45. Deng, R H, and Herro, M A, "DC-Free Coset Codes," *IEEE, Transactions on Information Theory*, Vol. 34, p. 786-792, July 1988.

46. Duman, T M, and Kurtas, E M, "Performance Bounds for High Rate Linear Codes Over Practical Response Channel," *IEEE, Transactions on Information Theory*, Vol. 47, no 3, p. 120, March 2001.

47. Dumer, I, "Nonbinary Double Error Correcting Codes Designed by Macro of Algebraic Varieties," *IEEE Transactions On Information Theory*, Vol. 41, No. 6, pp. 1657-1666, 1995.

48. Eerrou, C, Glaneux, A, and Thitimasjshima, P, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes (1)," Proceedings of IEEE, International Conference on Communications, Geneva, Switzerland, p. 1064-1070, May, 1993.

49. Elia M and Prati, G, "On the Complete Decoding of Binary Linear Code," *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 518-520, July 1985.

50. Elias, P, "Error Free Coding", *IEEE, Transactions on Information Theory*, Vol. 4, pp. 29-37, 1954.

51. Eric K H and Stephan G W, "Stream-Oriented Turbo Codes, A Stream Paradigm for Turbo Codes is Explored, Termed Stream-Oriented Turbo Codes," *IEEE Transactions on Information Theory*, Vol. 47 No. 5, pp. 1813-1831, July 2001.

52. Ericson T and Gyorfi, L, "Super Imposed Codes in R^n," *IEEE Transactions on Information Theory*, Vol. 34, no. 4, p. 877-880, July 1988.

53. Ericson. T, "Exponential Error Bounds for Random Codes in the Arbitrary Varying Channel," *IEEE, Transactions on Information Theory*, Vol. 31, No.1, pp. 42-48, January 1985.

54. Etzion T and Vardy, A, "Two-Dimensional Interleaving Schemes with Repetitions: Constructions and Bounds," ISIT 2000, Sorrento, Italy, June 2000.

55. Fano, R M, *Transmission of Information*. MIT Press, Cambridge, MA, 1961.

56. Farrell, P G and Hopkins, S J, "Burst Error Correcting Codes," *Radio Electron*, Vol. 52, no. 4, p. 182-192, 1982.

57. Feng, G L; Wei, W and Rao T N R, "New Double Byte Error Correcting Codes, in Memory Systems," Proceeding 1997, IEEE International Symposium on Information Theory, New York, 1997.

58. Feng, G L; Wei, W, Rao T N R and Tzeng, K K, "Simplified Understanding and Efficient Decoding of a Class of Algebraic Geometric Codes," *IEEE, Transactions on Information Theory*, Vol. 40, pp. 981-1002, 1994.

59. Forney, G D Jr., "Codes on Graphs: Normal Realizations ",*IEEE, Transactions on Information Theory*, Vol. 47, no 2, p. 520-548, February 2001.

60. Forney, G D Jr., "Codes on Graphs: Normal Realizations", *IEEE, Transactions on Information Theory*, Vol. 47, no 2, pp 520-548,Feburary 2001.

61. Forney, G D Jr., "Coding and its Application in Space Communication," *IEEE Spectrum*, pp. 47-58, 7 June 1970.

62. Forney, G D Jr., "Coset Codes – Part I: Introduction and Geometrical Classification", *IEEE, Transactions on Information Theory*, Vol. 34, no 5, pp 1123-1151,September 1988

63. Forney, G D Jr., "Coset Codes – Part II: Binary Lattices and Related Codes", *IEEE, Transactions on Information Theory*, Vol. 34, no 5, pp 1152-1187, September 1988

64. Forney, G D Jr., "On Decoding BCH Codes," *IEEE Transactions on Information Theory*, pp. 549-557, 1965.

65. Forney, G D Jr., *Coded Modulation for Band Limited Channels, IEEE Information Theory Society*, Newsletter, December 1990.

66. Forney, G D, "Burst Correcting Codes for Classic Bursty Channel," IEEE, Transaction on Communication, Vol. 19, p. 772-781, 1971.

67. Fossorier, M, Imai, H, Lin, S, and Poli, A, "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes," Proceedings of 13th International Symposium, AAECC-13, Springer-Verlag, Berlin, 1999.

68. Fu, F W, Klove, T, Luo, Y, and Wei, V K, "On the Svanstrom Bound for Ternary Constant-Weight Codes," *IEEE, Transactions on Information Theory*, Vol. 47, no 5, p. 2061-2064, July 2001.

69. Gallager, R G, "A Simple Derivation of Coding Theorem and Some Applications,: *IEEE, Transactions on Information Theory*, Vol. 11, pp. 3-8, 1965.

70. Gallager, R G, "Claude Shannon: A Retrospective on his life, Work and Impact (invited Paper)," *IEEE, Transactions on Information Theory*, Vol. 47, no 7, p. 2681-2695, Nov 2001.

71. Geman S, Cochanek, K, "Dynamic Programming and the Graphical Representation of Error-Correcting Codes:", *IEEE, Transactions on Information Theory*, Vol. 47, no 2, pp. 549-568, February 2001.

72. Gilbert, E N, "A Comparison of Signaling Alphabets," *Bell Systems Technical Journal*, Vol. 31, pp. 504-522, 1952.

73. Golay, M J E, "Notes on Digita1 Coding," Proc. *IEEE Transactions on Information Theory*, Vol. 37, pp. 437-444, 1949.

74. Goley, M J E, "Notes on Digital coding," Proceedings of IEEE, vol. 37, pp. 437-444, 1949.

75. Golomb, S W (eds), *Digital Communications with Space Applications*, Prentice Hall Englewood Cliffs, New Jersey, 1964.

76. Golomb, S W, "A General Formulation of Error Metrics," *IEEE Transactions Information Theory*, Vol. 15, pp. 425-426, 1969.

77. Gubmer, J A, "On the Deterministic Code Capacity of Multiple Asses Arbitrarily Varying Channel," *IEEE Transactions on Information Theory*, Vol. 36, No. 2, March 1990.

78. Guiliang, F; Xinuven W and Rao, T R N, "New Double Byte Error Correcting Codes for Memory System," *Proceeding of 1997 IEEE International Symposium on Information Theory*, pp. 260, July 1997.

79. Hada, Tand Kasahara, M, "Notes on a Construction of Error Correcting Codes," *Transactions of the Institute of Electronics, Information and Communication Engineers*, A Vol., J84- A, No. 4, pp. 543-52, Japan, April 2001.

80. Hagenauer, J, "The Turbo Principle: Tutorial Introduction and State of The Art," Proceedings International Symposium, Turbo Codes, Brest, France, p. 1-11, 1997.

81. Hall, E K and Wilson, S G, "Stream Oriented Turbo Codes", *IEEE, Transactions on Information Theory*, Vol. 47, no 5, p. 1813-1837, July 2001.

82. Hamming, R W, "Error Detecting and Error Correcting Codes," *Bell Systems Technical Journal*, Vol. 29, pp. 147-160, 1950.

83. Hamming, R W, *Coding and Information Theory*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, 1980.

84. Helleseth, T, Klove T and Levenshtein, V L, "On the Information Function of an Error Correcting Code," *IEEE Transactions on Information Theory*, Vol. 43, No. 2, pp. 549-57, March 1997.

85. Helstrom, C W, "SEC Codes for non-binary error correcting codes," *IEEE, Transactions on Information Theory*, Vol. 4, pp. 77-82, 1961.

86. Hill, R, *A First Course in Coding Theory*, Oxford Press, Oxford, 1986.

87. Hocquenghem, A, "A codes correctectures and de-erasures," Chiffers (Paris), Vol. 2, pp. 147-156, 1959.

88. Hoffman, D G, et. al., *Coding Theory The Essentials*, Marcel Dekker Inc., New York, 1991.

89. Hoholdt, T and Pellikaan, R, "On the Decoding of Algebraic Geometric Codes," *IEEE, Transactions on Information Theory*, Vol. 41, pp. 1589-1614, 1995.

90. Hoholdt, T, Lint, I H Van and Pellikaan, R, "Algebraic Geometry Codes", In *Handbook of Coding Theory*, Elsevier Science Publishers, Amsterdam, 1998.

91. Hutton, J F; Betsos, G A; Schaffer L and Mitkas, M P A, "Error Correcting Codes for Optical Engineering," *IEEE Transactions on Information Theory*, Vol. 28, Conf., pp.146-56, 5-6 August 1996.

92. Imai, H, "Two Dimensional Burst Correcting codes," *Electron Communication in Japan*, Vol. 55A, No. 8, p. 9-16, 1972.

93. Imai, H, ed. *Essentials of Error-Control Coding Techniques*, California: Academic Press US, 1990.

94. Jacoibus H W, Cornets D V and Dick E B, "Bounds and Construction for Binary Codes of Length Less Than 24 and Asymmetric Distance Less Than 6," *IEEE Transactions on Information Theory*, Vol. 34, No. 5, p. 1321-1332, September 1988.

95. Jeong, C K and Joo, E K J, "Trellis Multilevel, and Turbo Codes with DC-Free Characteristics," IEICE, Transactions on Fundamentals of Electronics, *Communications and Computer Sciences*, vol. E83-A, no. 12 p. 2706-2714, Japan, December, 2000.

96. Justesen, J, Paaske, E and Ballan, M, "Quasi Cyclic Unit Memory Convolutuional Codes," *IEEE, Transactions on Information Theory*, Vol. 36, No. 3, p. 540-547, May 1990.

97. Justesen, J; Larsen, K J; Elbrand J H, A Havemose and T Hoholdt, "Construction and Decoding of a Class of Algebraic Geometry

Codes," *IEEE, Transactions on Information Theory*, Vol. 35, pp.811-821, 1989.

98. Kabashima, Y, Murayama, T, and Saad, D, "Typical Performance of Gallager-Type Error Correcting Codes," *Physical Review Letters*, Vol. 84, No. 9, pp. 1255-1258, February 2000.

99. Kabatianskii, G, Krouk E and Smeets, B, "A digital Signature Scheme Based on Random Error Correcting Codes, Cryptography and Coding," *6th IMA International Conference Proceedings*, Springer-Verlog, Berlin, Germany, pp. 161-167, 1997.

100. Kanter, I and Saad, D, "Error Correcting Codes That Nearly Saturate Shannon's Bound," *Physical Review Letters*, Vol. 83, No. 13, pp. 2660-2663, September 1999.

101. Kasami, T, Lin S and Peterson, W W, "Polynomial Codes," *IEEE Transactions on Information Theory*, Vol. 14, pp. 807-814, 1968 and Vol. 16, pp. 635, 1970.

102. Kawabata, S., "Quantum Interleaver: Quantum Error Correction for Burst Error," *Journal of the Physical Society of Japan*, vol. 69, no. 11 p.3540-3543, Japan, November 2000.

103. Knuth, D E, "Efficient Balanced Codes," *IEEE Transactions on Information Theory*, Vol. 32, no. 1, p. 51-54, January 1986.

104. Kuhn, V, Dekorsy, A and Kammeyer, K.D, "Low Rate Channel Coding for CDMA systems," *AEU-International Journal of Electronics and Communications*, vol. 54 no. 6 p. 353-63, Germany 2000.

105. Labiod, H and Boutaba, R, "Performance Evaluation of Block Error-Correcting Codes for High Speed Wireless Communication Links," *Interoperable Communications Networks*, Vol. 2, No. 2-4, pp. 171-187, 1999.

106. Labiod, H, “Performance of Reed Solomon Error-Correcting Codes on Fading Channels,” *IEEE International Conference on Personal Wireless Communications, IEEE*, Piscataway, NJ, pp. 259-263, USA, 1999.

107. Lauer, G S, “Some Optimal Partial Unit Memory codes,” *IEEE, Transactions on Information Theory*, Vol. 25, p. 240-243, March 1979.

108. Lee, C Y, “Some Properties of Non-Binary Error Correcting Codes,” *IEEE, Transactions on Information Theory*, Vol. 4, p. 77-82, 1958.

109. Lee, L M, “Short Unit Memory Byte Oriented Binary Convolutional Code Having Maximal Free Distance,” *IEEE, Transactions on Information Theory*, Vol. 22, pp. 349-352, May 1976.

110. Leom, J S, “A Probabilistic Algorithm for Computing Minimum Weight of Large Error-Correcting Codes,” *IEEE Transactions on Information Theory*, Vol. 34, No. 5, pp. 1354-1300, September 1988.

111. Lin S and Daniel J C Jr., *‘Error Control Coding’ Fundamental Applications*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, 1983.

112. Lint, J H V, “Algebraic Geometric Codes in Coding Theory and Design Theory I,” *The IMA Volumes in Maths and Application*, Vol. 20, Springer Verlag, 1990.

113. Lint, J H V, *Introduction to Coding Theory*, Springer-Verlag, New York, 2000.

114. Lobstein A C and Wee G J M, “On Normal and Subnormal q-ary Codes,” *IEEE, Transactions on Information Theory*, Vol. 35, no 6, p. 1291-1295, November 1989.

115. Luby, M G, Mitzenmacher, M, Shokrallahi, M A and Spielman, D A, “Efficient Erasure Error-Correcting Codes,” *IEEE, Transactions on Information Theory*, Vol. 47, pp. 569-584, February 2001.

116. Lyppens, H, "Reed-Solomon Error Correction," *Dr. Dobb's Journal*, Vol. 22 No. Iss. 1, Miller Freeman, pp. 30-34 and pp. 80-82, January 1997.

117. MacKay, D J C, "Good Error-Correcting Codes Based on Very Sparse Matrices," *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 399-431, March 1999.

118. MacWilliams, F J, and Sloane, N J A, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1988.

119. Matsuki, H, Oono, T, Takanashi H and Tanaka, T, "An Error Control Scheme for High-Speed Data Communication by PHS," *NIT R & D*, Vol. 45, Iss., 11,
pp. 1079-1088, 1997.

120. Mattson, H F and Solomon, E, "A New Treatment of Bose-Choudhary Codes," J. Soc., Indust. Appl. Math, pp. 654-669, 1961.

121. McEliece, R J, Rodemich, E R, Rumsey, H C and Welch, L R, "New upper Bounds on the rate of a Code via the Delsarte-Macwilliams inequalities," *IEEE, Transactions on Information Theory*, Vol. 27, 1977.

122. O'reilly, J J, and Popplewell, A, "A Further Note on DC-Free Coset Codes," *IEEE, Transactions on Information Theory*, Vol. 36, No. 3, pp. 675-676, May 1990.

123. Ostergard, P R J, "New Results on Optimal Error-Correcting Codes," *Proceedings of the 1999 IEEE, Information Theory and Communications Workshop, IEEE*, Piscataway, NJ, pp. 120, June 1999.

124. Overveld, W M C J, "some construction on new burst error correcting codes," *IEEE, Transactions on Information Theory*, Vol. 33, no 1, p. 153, January, 1987.

125. Overweld, W M C J Van, "Some Constructions of New Burst Error Correcting Codes," *IEEE Transactions On Information Theory*, Vol. 33, No. 5, September, I987.

126. Park, D S, Kim, J D and Kim, Y S, "Error Block Detection Technique for Mobile Video Transmission," *Proceedings of the SPIE – The International Society for Optical Engineering*, Vol. 3024, Iss. Pt 2, pp. 1231-1240, USA, 1997.

127. Patapoutian, A, Shen, B Z, and McEwan, P A, "Event Error Control Codes and Their Applciations," *IEEE, Transactions on Information Theory*, Vol. 47, no 6, pp. 2595-2603, September 2001.

128. Pearlman W A, Jakatdar, P, "A Transform Tree code for Stationary Gaussian Sources," *IEEE Transactions on Information Theory*, Vol. 31, no. 6, pp. 761-768, November 1985.

129. Pellikaan, R, "On a Decoding Algorithm for Codes on Maximal Curves," *IEEE, Transactions on Information Theory*, Vol. 35, pp. 1228-1232, 1989.

130. Peresy, Lancek, Sehgal and Christian, "Trellis Coding," *IEEE* Press US, New York, 1997.

131. Peterson W W and Weldon, E J Jr., *Error Correcting Codes*, MIT Press, 1972.

132. Peterson, W W, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," *IEEE Transactions on Information Theory*, Vol. 6, pp. 459-470, 1960.

133. Ping, L, Huang, X and Phamdo, N, "Zigzag Codes and Concatenated Zigzag Codes," *IEEE Transactions on Information Theory*, Vol. 47, no. 2, p. 800-807, USA, February 2001.

134. Piret, P H, “Binary Codes for Compared Channels,” *IEEE, Transactions on Information Theory*, Vol. 31, No. 3, pp. 436-440, May 1985.

135. Piret, P H, *Convolutional Codes, An Algebraic Approach*, Cambridge, Mass, The MIT Press, 1988.

136. Pless, V, *Introduction to The theory of Error Correcting Codes*, John Wiley and Sons Inc., New York, 1989.

137. Plotkin, M, “Binary Codes with specified Minimum distance,” *IEEE, Transactions on Information Theory*, pp. 445-450, 1960.

138. Pollara, F, McEliece R J and Abdel-Ghaffar, K, “Finite State Codes,” *IEEE Transactions on Information Theory*, Vol. 34, no. 5, pp. 1083-89, September 1988.

139. Prasad A R and Seki, K, “Hybrid ARQ for IP Packet Transmission,” *IEEE, 6th International Conference on Universal Person Communications Record, Bridging the way to the 21st Century, ICUPC 1997*, Vol.2, pp. 531-535.

140. Pussolle, J, Seret, D and Dramards, D, *Integration Digital Communication Networks*, John Wiley, US, 1988.

141. Qubbermann, H G, “Cyclotomic Goppa Codes,” *IEEE, Transactions on Information Theory*, Vol.34, No. 5, p.1317-1320, September, 1988.

142. Rao, T R N and Fujiware, E, *Error Corrected Coding for Computer Systems*, Prentice Hall Englewood Cliff, New Jersey, 1989.

143. Reed I S and Chen, X, *Error Control Coding for Data Networks*, Kluwer Academic Publishers, Boston, 1999.

144. Reed I S, “A brief History of the Development of Error Correcting Codes,” *Computers and Mathematics with Applications*, Vol. 39, No. 11, pp. 89-93, June 2000.

145. Reed, I S, "Brief History of Computer and Error Correcting Codes and My Work, Gus Solomon, 1997," *IEEE Pacific PIM Conference on Communication, Computers and Signal Processing 1987-1997*, Vol. 2, pp 732-735, 1997.

146. Rhee, M Y, *Error Correcting Coding Theory*, McGraw Hill Publishing Company, New York, 1989.

147. Roos, C, "A New Lower Bound for the Minimum Distance of a Cyclic Code," *IEEE, Transactions on Information Theory*, Vol. 29, pp. 330-332, 1983.

148. Saleki, J A, Chung F K and Wei, V K, "Optical Orthogonal Codes: Design Analysis and Applications," *IEEE, Transactions on Information Theory*, Vol. 35, no. 3, pp. 595-604, May 1989.

149. San, T, "Interleaving for Extending the Performance of Error Correcting Codes in Communication Systems," *Electronic Product Design*, Vol. 21, No. 3, pp. C 15-18, March 2000.

150. Saowapa, K, Kaneko, H and Fujiwara, E, "Systematic Binary Deletion/Insertion Error Correcting Codes Capable of Correcting Random Bit Errors," IEICE Transactions on Fundamentals of Electronics, *Communications and Computer Sciences*, vol. E83-A, no. 12 p. 2699-705, Japan, December 2000.

151. Shannon, C E, "A Mathematical Theory of Communication," *Bell Systems Technical Journal*, 27, pp. 379-423, 623-656, 1948.

152. Sharma, B D and Dass, B K, "Extended Varshamov-Gilbert and Sphere Packing Bounds for Burst Correcting Codes," *IEEE, Transactions on Information Theory*, Vol. 20, p. 291-292, 1974.

153. Sharma, B D, and Goel, S N, "A Note on Bound for Burst Correcting Codes with Lee Weight Constraint," *Information and Control*, Vol.33, no. 3, p. 210-216, 1977.

154. Skorobogatov, A N and Vladut, S G, "On the Decoding of Algebraic Geometric Codes," *IEEE, Transactions on Information Theory*, Vol. 36, pp. 1051-1060, 1990.

155. Spielman, D A, "Linear Time Encodable and Decodable Error Correcting Codes," *IEEE Transactions on Information Theory*, Vol. 42, Iss 6, pp.1723-31, November, 1996.

156. Stoian, R and Stoicheseu, D A, "Decoding Algorithms for Erasure-Correcting Array Codes," *Studies in Informatics and Control*, vol.10, no.1 p.29-36, Romania, March 2001.

157. Thommesen, C and Justesen, J, "Bounds on Distance and Error Exponents of Unit Memory Codes," *IEEE, Transactions on Information Theory*, Vol. 29, p. 637-649, September 1983.

158. Thommesen, C, "Error Correcting Capabilities of Concatenated Codes with MDS Outer Codes on Memoryless Channels with Maximum Likehood Decoding," *IEEE Transactions On Information Theory*, Vol. 33, No. 5, September 1987.

159. Tietavainen, A and Perko, A, "There are no unknown perfect Binary codes," Ann. Univ. Tarku, Ser. A.1, pp. 3-10, 1971.

160. Tietavainen, A, "On the non existence of perfect codes or finite fields," SIAM J, Appl. Maths, Vol. 24, pp. 88-96, 1973.

161. Tilborg, H V, "On Error Correcting Balance Codes," *IEEE Transactions on Information Theory*, Vol. 35, No. 5, pp. 1091-1095, 1989.

162. Tsfasman, M A, Vladut, S G and Zink, T, "Modular Curves, Shimura Curves and Goppa Codes, Better than Varshamov Gilbert Bound," *Math*, Nachrichten, Vol. 109, pp. 21-28, 1982.

163. Ungerboeck, G, "Channel Coding with Multi-level Phase Signals," *IEEE, Transactions on Information Theory*, Vol. 28, pp. 55-67, 1982.

164. Ungerboeck, G, "Trellis Coded Modulation with Redundant Signal Sets, Part II: State of Art," *IEEE Communication Magazines*, Vol. 25, pp. 12-21, February, 1987.

165. Vashamov, R R, "Estimates of the number of signals in error correcting codes," Dokl, Akad, Nauk SSR, Vol. 117, pp. 739-741, 1957.

166. Veron, P, "Improved Identification Schemes based on Error Correcting Codes," *Application Algebra in Engineering Communication and Computing*, Vol.8, Iss. 1, Springer-Verlog, pp. 57-69, 1997.

167. Waddington, S and Pickavance, K, "Approaching the Shannon Limit in Digital Broadcasting," *SMPTE Journal*, Vol. 109,No. 9, pp. 729-733, September 2000.

168. Wang, W S and Blostein, S D, "Video Image Transmission Over Mobile Satellite Channels," *Signal Processing: Image Communication*, Vol. 16, no. 6, pp. 531-40, February 2001.

169. Wei, L F, "Trellis Coded Modulation with Multi-Dimensional, Constellation," *IEEE, Transactions on Information Theory*, Vol. 33, pp. 483-501, July 1987.

170. Wen Q and Yang Y, "Application of Error-Correcting Codes to the Construction of Boolean Functions of Cryptographic Signature," *Chinese Journal of Electronics*, vol. 8, No. 4, pp. 396-397, October 1999.

171. Wicker, S B, *Error control systems for digital communications and storage*, New Jersey, Prentice-Hall International, USA, 1995.

172. Wilson, J H, "Error Correcting Codes for a T-User Binary Adder Channel," *IEEE Transactions On Information Theory*, Vol. 34, No. 4, July 1988.

173. Wyner, A D, "Low Density Burst Correcting Burst Codes," *IEEE, Transactions on Information Theory*, Vol. 9, pp. 124, 1963.

174. Wyner, A D, and Ash R, "Analysis of Recurrent Coded," *IEEE, Transactions on Information Theory*, Vol. 9, pp. 143-156, 1963. ****

175. Xavier, S P E, *Statistical Theory of Communication*, New Age International (P) Ltd., New Delhi, 1997.

176. Ye, C and Yeung, R W, "Some Basic Properties of Fix-Free Codes", *Transactions on Information Theory*, Vol. 47, no 1, p. 72-87, January 2001.

177. Zhag, W and Wolf, J K, "A Class of Binary Burst Error Correcting Quasi Cyclic Codes," *IEEE, Transactions on Information Theory*, Vol. 34, no. 3, pp. 463-479, May 1988.

178. Zhang W and Wolf J K, "A Class of Binary Burst Error Correcting Quasi Cyclic Codes," *IEEE, Transactions on Information Theory*, Vol. 34, pp. 463-79, May 1980.

179. Zhang, Z, Chengming, T, "On the Construction Systematic tEC/AUED Codes," *IEEE, Transactions on Information Theory*, Vol 39, 1993.

180. Zorger, U K, "New Construction of Codes with Partial Unit Memory that are Based on Reed-Soloman Codes," *IEEE, Transactions on Information Theory*, Vol. 30, no. 4, pp. 303-306, 1995.

181. Zyablov, V.; Shavgulidze, S and Bossert, M., "On the Existence of Turbo- and Product-Type Codes which Asymptotically Meet the Gilbert-Varshamov Bound," ITG-Fachbericht no.159, pp. 71-74, VDE-Verlag, Germany 2000.